kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 AO Kaspersky Lab

Inhalt

Kaspersky Security Center 15.1 Hilfe

Neuerungen

Über Kaspersky Security Center

- Architektur
- Hard- und Softwarevoraussetzungen
  - Anforderungen an den Administrationsserver
  - Anforderungen an die Web Console
  - Anforderungen an Server für mobile Geräte
  - Anforderungen an die Verwaltungskonsole
  - Anforderungen an den Administrationsagenten
- Kompatible Anwendungen und Lösungen von Kaspersky
- Lizenzen und Funktionen von Kaspersky Security Center 15.1
- Über die Kompatibilität der Kaspersky Security Center-Komponenten
- Vergleich von Kaspersky Security Center: Windows-basiert vs. Linux-basiert
- Über die Kaspersky Security Center Cloud Console

Kaspersky Security Center 15.1

- Grundbegriffe
  - Administrationsserver
  - Hierarchie des Administrationsservers
  - Virtueller Administrationsserver
  - Server für mobile Geräte
  - Webserver
  - Administrationsagent
  - Administrationsgruppen
  - Verwaltetes Gerät
  - Nicht zugeordnetes Gerät
  - Administrator-Arbeitsplatz
  - Verwaltungs-Plug-in
  - Web-Plug-ins zur Verwaltung
  - Richtlinien
  - Richtlinienprofile
  - Aufgaben
  - Aufgabenumfang
  - Interaktion von Richtlinien und lokalen Programmeinstellungen
  - Verteilungspunkt
  - Verbindungs-Gateway
- Hauptinstallationsszenario
- Ports, die von Kaspersky Security Center verwendet werden
- Zertifikate für die Ausführung mit Kaspersky Security Center
  - Über die Zertifikate von Kaspersky Security Center
  - Über das Zertifikat des Administrationsservers
  - Anforderungen an benutzerdefinierte Zertifikate für deren Verwendung in Kaspersky Security Center
  - Szenario: Angeben des benutzerdefinierten Zertifikats des Administrationsservers

Zertifikats des Administrationsservers mittels Dienstprogramm klsetsrvcert ersetzen
Administrationsagenten mit dem Administrationsserver mittels Dienstprogramm klmover verbinden
Webserver-Zertifikat neu ausstellen
Schemata für Datenverkehr und Portnutzung
Administrationsserver und verwaltete Geräte im LAN
Primärer Administrationsserver im LAN und zwei sekundäre Administrationsserver
Administrationsserver im LAN, verwaltete Geräte im Internet und Verwendung eines Reverse-Proxys
Administrationsserver im LAN, verwaltete Geräte im Internet: Verwendung eines Verbindungs-Gateways
Administrationsserver in der DMZ, verwaltete Geräte im Internet
Interaktion der Komponenten von Kaspersky Security Center und der Sicherheitsanwendungen: weitere Informationen
Konventionen für die Interaktionsschemata
Administrationsserver und DBMS
Administrationsserver und Verwaltungskonsole
Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendung
Software-Upgrades auf dem Client-Gerät mithilfe des Verteilungspunkts
Hierarchie der Administrationsserver: primärer Administrationsserver und sekundärer Administrationsserver
Hierarchie der Administrationsserver mit sekundärem Administrationsserver in der demilitarisierten Zone
Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät
Administrationsserver und zwei Geräte in der DMZ: ein Verbindungs-Gateway und ein Client-Gerät
Administrationsserver und Kaspersky Security Center Web Console
Aktivierung und Verwaltung der Sicherheitsanwendung auf dem mobilen Gerät
Bewährte Verfahren zur Bereitstellung
Härtungsleitfaden
Bereitstellung des Administrationsservers
Verbindungssicherheit
Konten und Authentifizierung
Verwaltung des Schutzes des Administrationsservers
Verwaltung des Schutzes der Client-Geräte
Konfigurieren des Schutzes für verwaltete Programme
Wartung des Administrationsservers
Ereignisübertragung an Systeme von Dritten
Sicherheitsempfehlungen für Drittanbieter-Informationssysteme
Empfehlungen für die Verwendung von Kaspersky-Sicherheitsanwendungen
Vorbereitung der Bereitstellung
Planung der Bereitstellung für Kaspersky Security Center
Typische Vorgehensweisen der Bereitstellung
Informationen über die Planung der Verteilung von Kaspersky Security Center in einem Unternehmensnetzwerk
Struktur des Schutzes im Unternehmen auswählen
Typische Konfigurationen von Kaspersky Security Center
Typische Konfiguration: Einzelbüro
Typische Konfiguration: Mehrere größere Büros mit eigenen Administratoren
Typische Konfiguration: Mehrere kleine Remote-Büros
DBMS für den Administrationsserver auswählen
Den kumulativen Patches CU12 bei Verwendung von SQL Server 2019 als DBMS anwenden
MariaDB x64-Server für die Arbeit mit Kaspersky Security Center 15.1 konfigurieren
MySQL x64-Server für die Arbeit mit Kaspersky Security Center 15.1 konfigurieren
PostgresSQL- oder Postgres Pro-Server für die Arbeit mit Kaspersky Security Center 15.1 konfigurieren

Mobile Geräte mit installiertem Kaspersky Endpoint Security für Android verwalten
Internetzugriff für den Administrationsserver bereitstellen
Internetzugriff: Administrationsserver in einem lokalen Netzwerk
Zugriff aus dem Internet: Administrationsserver in der demilitarisierten Zone
Zugriff aus dem Internet: Administrationsagent als Verbindungs-Gateway in der demilitarisierten Zone
Über Verteilungspunkte
Anzahl der Datei-Deskriptoren für den klnagent-Dienst erhöhen
Anzahl und Konfiguration der Verteilungspunkte bestimmen
Hierarchie des Administrationsservers
Virtuelle Administrationsserver
Informationen zu Einschränkungen von Kaspersky Security Center
Netzwerkbelastung
Erstmalige Bereitstellung des Antiviren-Schutzes
Erstmaliges Update der Antiviren-Datenbanken
Synchronisierung des Clients mit dem Administrationsserver
Zusätzliches Update der Antiviren-Datenbanken
Verarbeitung von Ereignissen der Clients durch Administrationsserver
Datenverkehr in 24 Stunden
Vorbereitung auf die Verwaltung mobiler Geräte
iOS MDM-Server
Typische Konfiguration: Kaspersky Device Management für iOS in der DMZ
Typische Konfiguration: iOS MDM-Server im lokalen Netzwerk des Unternehmens
Mobile Geräte mit installiertem Kaspersky Endpoint Security für Android verwalten
Informationen zur Leistungsfähigkeit des Administrationsservers
Einschränkungen der Verbindung mit dem Administrationsserver
Ergebnisse der Leistungstests des Administrationsservers
Ergebnisse der Leistungstests des KSN-Proxyservers
Netzwerkeinstellungen zur Interaktion mit externen Diensten
Softwareverteilung für den Administrationsagenten und die Sicherheitsanwendung
Erstmalige Bereitstellung
Anpassen der Einstellungen der Installer
Installationspakete
Eigenschaften des MSI-Installers und der Transformationsdateien
Bereitstellung mithilfe von Drittanbieter-Tools zur Remote-Installation von Apps
Über Aufgaben zur Remote-Installation in Kaspersky Security Center
Bereitstellung durch Erstellung und Verteilung eines Geräte-Images
Fehlerhaftes Kopieren eines Festplatten-Images
Bereitstellung mithilfe des Mechanismus der Gruppenrichtlinien von Microsoft Windows
Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center
Start der von Kaspersky Security Center gebildeten autonomen Pakete
Funktion zur manuellen Installation von Apps
Eine MST-Datei erstellen
Remote-Installation von Apps auf Geräte mit installiertem Administrationsagenten
Verwaltung des Neustarts von Geräten in der Aufgabe zur Remote-Installation
Zweckdienlichkeit des Datenbanken-Updates im Installationspaket der Sicherheitsanwendung
Verwendung von Tools zur Remote-Installation der Apps von Kaspersky Security Center für den Start von beliebigen ausführbaren Dateien auf den verwalteten Geräten

Monitoring der Bereitstellung
Anpassen der Einstellungen der Installer
Allgemeine Informationen
Installation im Silent-Modus (mit Antwortdatei)
Installation des Administrationsagenten im Silent-Modus (ohne Antwortdatei)
Teilweises Anpassen der Installationseinstellungen durch setup.exe
Installationseinstellungen für den Administrationsserver
Installationseinstellungen für den Administrationsagenten
Virtuelle Infrastruktur
Empfehlungen zur Senkung der Belastung auf den virtuellen Maschinen
Unterstützung von dynamischen virtuellen Maschinen
Unterstützung des Kopierens von virtuellen Maschinen
Unterstützung des Rollbacks des Dateisystems für Geräte mit Administrationsagent
Lokale Installation von Programmen
Lokale Installation des Administrationsagenten
Installation des Administrationsagenten im Silent-Modus
Administrationsagent für Linux im Silent-Modus installieren (mit einer Antwort-Datei)
Ein Gerät auf dem Astra Linux im Modus der abgeschlossenen Softwareumgebung ausgeführt wird für die Installation des Administrationsagenten vorbereiten
Administrationsagent für Linux im interaktiven Modus installieren
Lokale Installation des Plug-ins für die Programmverwaltung
Programme im Silent-Modus installieren
Programme mithilfe autonomer Installationspakete installieren
Einstellungen des Installationspakets des Administrationsagenten
Anzeigen der Datenschutzrichtlinie
Bereitstellung der Systeme zur Verwaltung mobiler Geräte
Bereitstellung des Verwaltungssystems mithilfe des iOS MDM-Protokolls
Installation des iOS MDM-Servers
iOS MDM-Server im Silent-Modus installieren
Schemata der Bereitstellung eines iOS MDM-Servers
Vereinfachtes Schema der Bereitstellung
Schema der Bereitstellung unter Verwendung der erzwungenen Delegierung Kerberos (KCD)
APNs-Zertifikat anfordern
Update des APNs-Zertifikats
Das Reservezertifikat des iOS MDM-Servers konfigurieren
APNs-Zertifikat auf dem iOS MDM-Server installieren
Einstellungen für den Zugriff auf den Dienst Apple Push Notification
Allgemeines Zertifikat ausstellen und auf dem mobilen Gerät installieren
KES-Gerät zur Liste der verwalteten Geräte hinzufügen
Verbindung von KES-Geräten mit dem Administrationsserver
Direkte Verbindung der Geräte mit dem Administrationsserver
Anschlussschema für KES-Geräte mit dem Server unter Verwendung der erzwungenen Delegierung Kerberos (KCD)
Verwendung von Firebase Cloud Messaging
Integration in die Public-Key-Infrastruktur
Kaspersky Security Center Webserver

Kaspersky Security Center installieren
- Vorbereitung der Installation
- Benutzerkonten für die Arbeit mit DBMS
  - Benutzerkonten für die Arbeit mit SQL Server konfigurieren (Windows-Authentifizierung)
  - Benutzerkonten für die Arbeit mit SQL Server konfigurieren (SQL Server-Authentifizierung)
  - Benutzerkonten für die Arbeit mit MySQL und MariaDB konfigurieren
  - In MySQL und MariaDB-DBMS Daten aus einem freigegebenen Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschieben
  - Benutzerkonten für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren
- Szenario: Authentifizierung von Microsoft SQL Server
- Szenario: Authentifizierung am MySQL-Server
- Szenario: Authentifizierung am PostgreSQL-Server
- Installationsempfehlungen für den Administrationsserver
  - Benutzerkonten für die Dienste des Administrationsservers auf dem Failover-Cluster erstellen
  - Den freigegebenen Ordner angeben
  - Remote-Installation über den Administrationsserver mithilfe von Gruppenrichtlinien des Active Directory
  - Remote-Installation über den Versand des UNC-Pfads an das autonome Paket
  - Update aus dem freigegebenen Ordner des Administrationsservers
  - Betriebssystem-Images installieren
  - Adresse des Administrationsservers angeben
- Standardinstallation
  - Schritt 1. Anzeigen des Lizenzvertrags und der Datenschutzrichtlinie
  - Schritt 2. Installationsart auswählen
  - Schritt 3. Kaspersky Security Center Web Console installieren
  - Schritt 4. Auswählen der Netzwerkgröße
  - Schritt 5. Auswählen der Datenbank
  - Schritt 6. Konfigurieren des SQL-Servers
  - Schritt 7. Auswählen eines Authentifizierungsmodus
  - Schritt 8. Entpacken und Installieren der Dateien auf der Festplatte
- Benutzerdefinierte Installation
  - Schritt 1. Anzeigen des Lizenzvertrags und der Datenschutzrichtlinie
  - Schritt 2. Installationsart auswählen
  - Schritt 3. Auswählen der zu installierenden Komponenten
  - Schritt 4. Kaspersky Security Center Web Console installieren
  - Schritt 5. Auswählen der Netzwerkgröße
  - Schritt 6. Auswählen der Datenbank
  - Schritt 7. Konfigurieren des SQL-Servers
  - Schritt 8. Auswählen eines Authentifizierungsmodus
  - Schritt 9. Auswählen des Benutzerkontos für den Start des Administrationsservers
  - Schritt 10. Auswählen des Benutzerkontos für das Ausführen der Dienste von Kaspersky Security Center
  - Schritt 11. Festlegen eines gemeinsamen Ordners
  - Schritt 12. Konfigurieren der Verbindung zum Administrationsserver
  - Schritt 13. Festlegen der Adresse des Administrationsservers
  - Schritt 14. Adresse des Administrationsservers für die Verbindung mit mobilen Geräten
  - Schritt 15. Plug-ins für die Programmverwaltung wählen
  - Schritt 16. Entpacken und Installieren der Dateien auf der Festplatte

Kaspersky Security Center Failover-Cluster bereitstellen
Szenario: Ein Kaspersky Security Center Failover-Cluster bereitstellen
Über das Kaspersky Security Center Failover-Cluster
Einen Dateiserver für ein Kaspersky Security Center Failover-Cluster vorbereiten
Knoten für ein Kaspersky Security Center Failover-Cluster vorbereiten
Kaspersky Security Center auf den Knoten des Kaspersky Security Center Failover-Clusters installieren
Cluster-Knoten manuell starten und beenden
Installation des Administrationsservers in einem Windows Server Failover-Cluster
Schritt 1. Anzeigen des Lizenzvertrags und der Datenschutzrichtlinie
Schritt 2. Auswählen des Installationstyps in dem Cluster
Schritt 3. Angeben des Namens des virtuellen Administrationsservers
Schritt 4. Angeben der Netzwerkdetails des virtuellen Administrationsservers
Schritt 5. Angeben einer Clustergruppe
Schritt 6. Auswählen eines Cluster-Datenspeichers
Schritt 7. Angeben eines Kontos für die Remote-Installation
Schritt 8. Auswählen der zu installierenden Komponenten
Schritt 9. Auswählen der Netzwerkgröße
Schritt 10. Auswählen der Datenbank
Schritt 11. Konfigurieren des SQL-Servers
Schritt 12. Auswählen eines Authentifizierungsmodus
Schritt 13. Auswählen des Benutzerkontos für den Start des Administrationsservers
Schritt 14. Auswählen des Benutzerkontos für das Ausführen der Dienste von Kaspersky Security Center
Schritt 15. Festlegen eines gemeinsamen Ordners
Schritt 16. Konfigurieren der Verbindung zum Administrationsserver
Schritt 17. Festlegen der Adresse des Administrationsservers
Schritt 18. Adresse des Administrationsservers für die Verbindung mit mobilen Geräten
Schritt 19. Entpacken und Installieren der Dateien auf der Festplatte
Installation des Administrationsservers im Silent-Modus
Verwaltungskonsole auf dem Administrator-Arbeitsplatz installieren
Änderungen im System nach der Installation von Kaspersky Security Center
Programmdeinstallation
Über das Upgrade von Kaspersky Security Center
Update der vorherigen Version von Kaspersky Security Center
Kaspersky Security Center auf den Knoten des Kaspersky Security Center Failover-Clusters aktualisieren
Kaspersky Security Center auf den Knoten eines Microsoft-Failover-Clusters aktualisieren
Erstkonfiguration von Kaspersky Security Center
Härtungsleitfaden
Der Schnellstartassistent für den Administrationsserver
Über den Schnellstartassistenten
Start des Schnellstartassistenten für den Administrationsserver
Schritt 1. Konfigurieren eines Proxyservers
Schritt 2. Auswählen der Methode zur Programmaktivierung
Schritt 3. Auswählen der Schutzbereiche und Betriebssysteme
Schritt 4. Auswählen der Plug-ins für verwaltete Programme
Schritt 5. Herunterladen der Programmpakete Erstellen der Installationspakete
Schritt 6. Konfigurieren von Kaspersky Security Network
Schritt 7. Konfigurieren von E-Mail-Benachrichtigungen

Schritt 8. Konfigurieren der Update-Verwaltung
Schritt 9. Konfigurieren des ersten Schutzes
Schritt 10. Verbinden mobiler Geräte
Schritt 11. Herunterladen von Updates
Schritt 12. Suchen von Geräten
Schritt 13. Abschließen des Schnellstartassistenten
Verbindung der Verwaltungskonsole mit dem Administrationsserver anpassen
Die Internetzugriffseinstellungen für den Administrationsserver konfigurieren
Verbinden mobiler Geräte
Szenario: Verbinden von mobilen Geräten mittels Verbindungs-Gateway
Szenario: Verbinden von mobilen Geräten mittels einem sekundären Administrationsserver in der DMZ
Über das Verbinden mobiler Geräte
Verbinden von externen Desktop-Geräten mit dem Administrationsserver
Über Verbindungsprofile für mobile Benutzer
Erstellen eines Verbindungsprofils für mobile Benutzer
Über das Umschalten eines Administrationsagenten auf einen anderen Administrationsserver
Erstellen der Regel für die Umstellung des Administrationsagenten gemäß dem Netzwerkspeicherort
Ereignisbenachrichtigungen
Benachrichtigungseinstellungen für Ereignisse anpassen
Verteilung von Benachrichtigungen prüfen
Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei
Kommunikation mit TLS verschlüsseln
Schnittstelle konfigurieren
Geräte im Netzwerk finden
Szenario: Netzwerkgeräte finden
Nicht zugeordnete Geräte
Suchen von Geräten
Windows-Netzwerkabfrage
Abfrage der Active Directory
IP-Bereiche abfragen
Zeroconf-Abfrage
Arbeit mit Windows-Domänen. Domäneneinstellungen anzeigen und ändern
Aufbewahrungsregeln für nicht zugeordnete Geräte anpassen
Arbeiten mit IP-Bereichen
IP-Bereich erstellen
Einstellungen eines IP-Bereichs anzeigen und ändern
Active Directory Gruppen. Gruppeneinstellungen anzeigen und ändern
Regeln für das automatische Verschieben von Geräten in Administrationsgruppen erstellen
Dynamischen VDI-Modus auf Client-Geräten verwenden
Dynamischen VDI-Modus in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren
Geräte suchen, die zu VDI gehören
Geräte, die zu VDI gehören, in eine Administrationsgruppe verschieben
Arbeitsgerätebestand
Informationen über neue Geräte hinzufügen
Kriterien zur Erkennung von Unternehmensgeräten anpassen
Benutzerdefinierte Felder anpassen

Lizenzierung
Ereignisse bei Überschreitung der Lizenzbeschränkung
Über die Lizenzierung
Über die Lizenz
Über den Endbenutzer-Lizenzvertrag
Über das Lizenzzertifikat
Über den Lizenzschlüssel
Über die Schlüsseldatei
Über das Abonnement
Über den Aktivierungscode
Vereinbarung mit einem Endbenutzer-Lizenzvertrag widerrufen
Über die Bereitstellung von Daten
Varianten der Lizenzierung von Kaspersky Security Center
Besonderheiten der Lizenzverwaltung für Kaspersky Security Center und die verwalteten Programme
Kaspersky-Anwendungen. Zentralisierte Bereitstellung
Sicherheitsanwendungen von Drittanbietern ersetzen
Anwendungen mit der Aufgabe zur Remote-Installation installieren
Programm auf ausgewählten Geräten installieren
Programm auf den Client-Geräten einer Administrationsgruppe installieren
Programme mit Gruppenrichtlinien des Active Directory installieren
Remote-Installation von Anwendungen auf macOS-Geräten
Anwendungen auf sekundären Administrationsservern installieren
Programme mit dem Assistenten für Remote-Installationen installieren
Umgang mit Verwaltungs-Plug-ins
Bericht über die Bereitstellung des Schutzes anzeigen
Remote-Deinstallation von Programmen
Remote-Deinstallation eines Programms von den Client-Geräten einer Administrationsgruppe
Remote-Deinstallation eines Programms von den gewählten Geräten
Verwendung von Installationspaketen
Installationspaket erstellen
Autonome Installationspakete erstellen
Erstellen benutzerdefinierter Installationspakete
Eigenschaften von benutzerdefinierten Installationspaketen anzeigen und bearbeiten
Installationspaket des Administrationsagenten aus dem Programmpaket von Kaspersky Security Center beziehen
Installationspakete an sekundäre Administrationsserver verteilen
Installationspakete mithilfe von Verteilungspunkten verteilen
Daten über die Ergebnisse der Programminstallation an Kaspersky Security Center übertragen
Die KSN-Proxy Server-Adresse für Installationspakete festlegen
Aktuelle Versionen der Programme downloaden
Ein Windows-Gerät für die Remote-Installation vorbereiten
Ein Linux-Gerät vorbereiten und den Administrationsagenten auf einem Linux-Gerät remote installieren
Ein Gerät mit SUSE Linux Enterprise Server 15 für die Installation des Administrationsagenten vorbereiten
Ein Gerät mit dem Betriebssystem macOS für die Remote-Installation des Administrationsagenten vorbereiten
Kaspersky-Anwendungen: Lizenzierung und Aktivierung
Lizenzierung der verwalteten Programme
Informationen zu verwendeten Lizenzschlüsseln anzeigen
Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen

Lizenzschlüssel des Administrationsservers entfernen
Lizenzschlüssel auf Client-Geräte verteilen
Lizenzschlüssel automatisch verteilen
Bericht über die Nutzung von Lizenzschlüsseln erstellen und anzeigen
Informationen zu den Lizenzschlüsseln des Programms anzeigen
Eine Lizenzschlüsseldatei exportieren
Netzwerkschutz konfigurieren
Szenario: Netzwerkschutz konfigurieren
Richtlinien einrichten und verwalten: geräteorientierte Herangehensweise
Geräteorientierte und benutzerorientierte Methode der Sicherheitsverwaltung
Richtlinie für Kaspersky Endpoint Security manuell konfigurieren
Einstellungen der Richtlinie im Abschnitt "Erweiterter Schutz"
Einstellungen der Richtlinie im Abschnitt "Basisschutz"
Einstellungen der Richtlinie im Abschnitt "Allgemeine Einstellungen"
Einstellungen der Richtlinie im Abschnitt "Konfiguration von Ereignissen"
Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren
Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security
Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen
Manuelle Konfiguration der Gruppenaufgabe zur Installation von Updates und zum Schließen von Schwachstellen
Maximalen Anzahl an Ereignissen in der Ereignis-Datenverwaltung festlegen
Die maximale Speicherdauer für Informationen über behobenen Schwachstellen festlegen
Aufgaben verwalten
Aufgaben erstellen
Aufgabe des Administrationsservers erstellen
Aufgabe für eine Reihe von Geräten erstellen
Lokale Aufgaben erstellen
Vererbte Gruppenaufgabe im Arbeitsbereich der untergeordneten Gruppe darstellen
Geräte vor Ausführung einer Aufgabe automatisch einschalten
Gerät nach der Ausführung einer Aufgabe automatisch ausschalten
Zeitlimit für Aufgabenausführung festlegen
Aufgaben exportieren
Aufgaben importieren
Aufgaben konvertieren
Aufgaben manuell starten und beenden
Aufgaben manuell fortsetzen und anhalten
Aufgabenausführung überwachen
Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen
Filter für die Informationen über die Ergebnisse der Aufgabenausführung konfigurieren
Ändern der Aufgabe Rollback der Änderungen
Vergleich von Aufgaben
Die Benutzerkonten für den Aufgabenstart
Verlauf der Aufgabenausführung exportieren
Assistent zum Ändern der Aufgabenkennwörter
Schritt 1. Anmeldedaten angeben
Schritt 2. Auszuführenden Vorgang auswählen
Schritt 3. Ergebnisse anzeigen
Hierarchie der Administrationsgruppen erstellen, die dem virtuellen Administrationsserver untergeordnet sind

Richtlinien und Richtlinienprofile
Richtlinienhierarchie, Verwendung von Richtlinienprofilen
Hierarchie der Richtlinien
Richtlinienprofile
Vererbung von Richtlinieneinstellungen
Richtlinien verwalten
Richtlinie erstellen
Vererbte Richtlinie in der untergeordneten Gruppe darstellen
Richtlinien aktivieren
Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren
Richtlinie für mobile Benutzer übernehmen
Richtlinie ändern. Rollback der Änderungen
Vergleich von Richtlinien
Diagramm für den Status der Richtlinienverteilung anzeigen
Richtlinien löschen
Richtlinien kopieren
Richtlinien exportieren
Richtlinien importieren
Richtlinien konvertieren
Richtlinienprofile verwalten
Richtlinienprofil erstellen
Richtlinienprofil ändern
Richtlinienprofil löschen
Regeln für die Aktivierung des Richtlinienprofils erstellen
Verschiebungsregeln für Geräte
Klonen von Regeln für das Verschieben von Geräten
Software-Kategorisierung
Erforderliche Bedingungen für die Installation von Programmen auf den Geräten des Kundenunternehmens
Lokale Einstellungen des Programms anzeigen und ändern
Kaspersky Security Center und verwaltete Programme aktualisieren
Szenario: Datenbanken und Programme von Kaspersky regelmäßig aktualisieren
Über das Aktualisieren der Datenbanken, Software-Module und Programme von Kaspersky
Über die Verwendung von Diff-Dateien zum Update von Kaspersky-Datenbanken und Software-Modulen
Funktion zum Herunterladen von Diff-Dateien aktivieren
Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen
Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen
Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers anpassen
Heruntergeladene Updates prüfen
Konfiguration der Prüfungsrichtlinien und Hilfsaufgaben
Heruntergeladene Updates anzeigen
Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren
Autonomes Modell für den Download von Updates
Autonomes Modell für den Download von Updates aktivieren und deaktivieren
Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center
Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren

Updates automatisch verteilen
Updates automatisch auf Client-Geräte verteilen
Updates automatisch an sekundäre Administrationsserver verteilen
Verteilungspunkte automatisch zuweisen
Gerät manuell zum Verteilungspunkt bestimmen
Gerät aus der Liste der Verteilungspunkte entfernen
Updates mittels Verteilungspunkten herunterladen
Software-Updates aus der Datenverwaltung löschen
Patchinstallation für eine Kaspersky-Anwendung im Cluster-Modell
Drittanbieter-Programme auf Client-Geräten verwalten
Über Anwendungen von Drittanbietern
Updates für Drittanbieter-Programme installieren
Szenario: Aktualisieren von Software von Drittanbietern
Informationen zu verfügbaren Updates für Anwendungen von Drittanbietern anzeigen
Programm-Updates genehmigen und ablehnen
Windows-Updates mit dem Administrationsserver synchronisieren
Schritt 1. Festlegen, ob der Datenverkehr reduziert werden soll
Schritt 2. Anwendungen
Schritt 3. Update-Kategorien
Schritt 4. Update-Sprachen
Schritt 5. Auswählen des Kontos für Aufgabenausführung
Schritt 6. Konfigurieren des Zeitplans für den Aufgabenstart
Schritt 7. Festlegen des Aufgabennamens
Schritt 8. Abschließen der Aufgabenerstellung
Manuelle Installation von Updates auf Geräte
Windows-Updates in der Richtlinie des Administrationsagenten anpassen
Schwachstellen in Drittanbieter-Anwendungen schließen
Szenario: Finden und Schließen von Schwachstellen in Programmen von Drittanbietern
Über die Suche nach und das Schließen von Software-Schwachstellen
Informationen über Schwachstellen in Programmen anzeigen
Statistik über Schwachstellen auf verwalteten Geräten anzeigen
Schwachstellensuche in Programmen
Schließen von Schwachstellen in Programmen
Schwachstellen in einem isolierten Netzwerk schließen
Szenario: Schwachstellen in Drittanbieter-Programmen in einem isolierten Netzwerk beheben
Über das Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk
Administrationsserver mit Internetzugang konfigurieren, um Schwachstellen in einem isolierten Netzwerk zu schließen
Isolierte Administrationsserver konfigurieren, um Schwachstellen in einem isolierten Netzwerk zu schließen
Übertragung von Patches und Installation von Updates in einem isolierten Netzwerk
Option zum Übertragen von Patches und Installieren von Updates in einem isolierten Netzwerk deaktivieren
Ignorieren von Schwachstellen in Programmen
Auswählen von Benutzerkorrekturen für Schwachstellen in Programmen von Drittanbietern
Regeln zur Installation von Updates
Programmgruppen
Programmkontrolle zur Verwaltung ausführbarer Dateien verwenden
Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen
Erstellen von Programmkategorien für Richtlinien von Kaspersky Endpoint Security für Windows

Manuell zu erweiternde Programmkategorie erstellen
Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen
Erstellen einer Programmkategorie mit ausführbaren Dateien aus einem bestimmten Ordner
Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen
Verwaltung des Programmstarts auf Client-Geräten anpassen
Ergebnisse der statischen Analyse der Regeln für den Start ausführbarer Dateien anzeigen
Programm-Registry anzeigen
Startzeit der Software-Inventur ändern
Über die Verwaltung von Lizenzschlüsseln von Drittanbieter-Programmen
Lizenzierte Programmgruppen erstellen
Verwaltung von Lizenzschlüsseln für lizenzierte Programmgruppen
Inventarisierung der ausführbaren Dateien
Informationen über ausführbare Dateien anzeigen
Überwachung und Berichterstattung
Szenario: Überwachung und Berichterstattung
Farbliche Kennzeichnungen und protokollierte Ereignissen in der Verwaltungskonsole überwachen
Arbeiten mit Berichten, Statistiken und Benachrichtigungen
Arbeiten mit Berichten
Berichtsvorlage erstellen
Eigenschaften von Berichtsvorlagen anzeigen und bearbeiten
Erweitertes Filterformat in Berichtsvorlagen
Filter in das erweiterte Filterformat konvertieren
Erweiterten Filter anpassen
Berichte erstellen und anzeigen
Bericht speichern
Aufgabe zum Berichtsversand anlegen
Schritt 1. Auswählen des Aufgabentyps
Schritt 2. Auswählen des Berichtstyps
Schritt 3. Vorgänge mit Berichten
Schritt 4. Auswählen des Kontos für Aufgabenausführung
Schritt 5. Konfigurieren eines Aufgabenzeitplans
Schritt 6. Festlegen des Aufgabennamens
Schritt 7. Abschließen der Aufgabenerstellung
Arbeiten mit statistischen Daten
Benachrichtigungseinstellungen für Ereignisse anpassen
Zertifikat für SMTP-Server erstellen
Ereignisauswahlen
Ereignisauswahl anzeigen
Einstellungen für Ereignisauswahl anpassen
Ereignisauswahl erstellen
Ereignisauswahl in eine Textdatei exportieren
Ereignisse aus einer Auswahl löschen
Programme auf Anfrage von Benutzern zu Ausschlüssen hinzufügen
Geräteauswahlen
Geräteauswahl anzeigen
Einstellungen einer Geräteauswahl anpassen
Einstellungen einer Geräteauswahl in eine Datei exportieren

Geräteauswahl erstellen
Geräteauswahl mit importierten Einstellungen erstellen
Geräte in der Auswahl aus Administrationsgruppen löschen
Überwachung der Installation und Deinstallation von Anwendungen
Ereignisse der Komponenten von Kaspersky Security Center
Datenstruktur der Beschreibungen von Ereignistypen
Ereignisse des Administrationsservers
Ereignisse des Administrationsservers: Kritisch
Ereignisse des Administrationsservers: Funktionsfehler
Ereignisse des Administrationsservers: Warnung
Ereignisse des Administrationsservers: Information
Ereignisse des Administrationsagenten
Administrationsagent: Ereignisse bei Funktionsfehlern
Ereignisse des Administrationsagenten: Warnung
Ereignisse des Administrationsagenten: Information
Ereignisse des iOS MDM-Servers
Ereignisse des iOS MDM-Servers: Funktionsfehler
Ereignisse des iOS MDM-Servers: Warnung
Ereignisse des iOS MDM-Servers: Information
Häufige auftretende Ereignisse blockieren
Über das Blockieren von häufig auftretenden Ereignissen
Das Blockieren häufig auftretender Ereignissen verwalten
Die Blockade häufig auftretender Ereignisse aufheben
Liste mit häufigen auftretenden Ereignissen in eine Datei exportieren
Kontrolle über den Status der virtuellen Maschinen
Status des Antiviren-Schutzes mit Systemregistrierung verfolgen
Maßnahmen anzeigen und konfigurieren, wenn Geräte als inaktiv angezeigt werden
Kaspersky-Mitteilungen deaktivieren
Verteilungspunkte und Verbindungs-Gateways anpassen
Typische Konfiguration von Verteilungspunkten: Einzelbüro
Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros
Zuweisen eines verwalteten Geräts als Verteilungspunkt
Verbinden eines Linux-Gerätes als Gateway in einer demilitarisierten Zone
Verbinden eines Linux-Geräts mit dem Administrationsserver über ein Verbindungs-Gateway
Hinzufügen eines Verbindungs-Gateways als Verteilungspunkt innerhalb der DMZ
Verteilungspunkte automatisch zuweisen
Administrationsagenten lokal auf dem als Verteilungspunkt ausgewählten Gerät installieren
Verteilungspunkt als Verbindungs-Gateway verwenden
Weitere IP-Bereiche zur Liste mit Bereichen hinzufügen, die von einem Verteilungspunkt abgefragt werden
Verteilungspunkt als Push-Server verwenden
Weitere Routinearbeiten
Administrationsserver verwalten
Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen
Verbindung mit dem Administrationsserver herstellen und zwischen Administrationsservern wechseln
Zugriffsberechtigungen für den Administrationsserver und dessen Objekte
Bedingungen für das Herstellen einer Internetverbindung mit dem Administrationsserver

Geschützte Verbindung mit dem Administrationsserver einrichten
Authentifizierung des Administrationsservers beim Verbinden des Geräts
Authentifizierung des Administrationsservers beim Verbindungsaufbau mit der Verwaltungskonsole
Eine Allow-Liste von IP-Adressen für die Verbindung mit dem Administrationsserver konfigurieren
Klscflag-Tool zum Schließen von Port 13291 verwenden
Verbindung mit dem Administrationsserver trennen
Administrationsserver zur Konsolenstruktur hinzufügen
Administrationsserver aus der Konsolenstruktur entfernen
Hinzufügen eines virtuellen Administrationsservers zur Konsolenstruktur hinzufügen
Benutzerkonto des Administrationsserver-Dienstes wechseln. Tool klsrvswch
DBMS-Anmeldedaten ändern
Den freigegebenen Ordner des Administrationsservers ändern
Probleme mit den Knoten des Administrationsservers lösen
Einstellungen des Administrationsservers anzeigen und ändern
Allgemeine Einstellungen des Administrationsservers konfigurieren
Schnittstelleneinstellungen der Verwaltungskonsole
Ereignisse auf dem Administrationsserver verarbeiten und speichern
Protokoll der Verbindungen zum Administrationsserver anzeigen
Eintreten von Virenangriffen kontrollieren
Datenverkehr begrenzen
Webserver-Einstellungen anpassen
Arbeit mit internen Benutzern
Verschieben ins Backup und Wiederherstellen der Einstellungen des Administrationsservers
Nutzung von Momentaufnahmen des Dateisystems zur Verkürzung der Dauer des Verschiebens ins Backup
Ein Gerät mit dem Administrationsserver ist ausgefallen
Die Einstellungen des Administrationsservers oder der Datenbank sind beschädigt
Daten des Administrationsservers sichern und wiederherstellen
Aufgabe zum Anlegen eines Backups der Daten des Administrationsservers
Tool zur Sicherung- und Wiederherstellung der Daten (klbackup)
Anlegen und Wiederherstellen eines Daten-Backups im interaktiven Modus
Daten im Silent-Modus sichern, kopieren und wiederherstellen
Das klbackup-Tool verwenden, um verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers zu stellen
Daten des Administrationsservers bei Verwendung von MySQL oder MariaDB sichern und wiederherstellen
Erstellen und Wiederherstellen eines Backups der Daten des Administrationsservers optimieren
Administrationsserver auf anderes Gerät übertragen
Konflikte zwischen mehreren Administrationsservern vermeiden
Administrationsgruppen verwalten
Administrationsgruppen anlegen
Administrationsgruppen verschieben
Deleting administration groups
Administrationsgruppenstruktur automatisch anlegen
Programme automatisch auf Geräten einer Administrationsgruppe installieren
Client-Geräte verwalten
Client-Geräte mit dem Administrationsserver verbinden
Client-Gerät manuell mit Administrationsserver verbinden. Tool klmover
Verbindung des Client-Geräts mit dem Administrationsserver tunneln

Remotedesktopverbindung mit dem Client-Gerät herstellen
Eine Verbindung mit Windows-Client-Geräten herstellen
Eine Verbindung mit macOS-Client-Geräten herstellen
Verbindung mit den Client-Geräten über die Windows Desktopfreigabe herstellen
Einstellungen für den Neustart des Client-Geräts
Überwachung der Aktionen auf einem Remote-Client-Gerät
Verbindung des Client-Geräts mit dem Administrationsserver prüfen
Verbindung des Client-Geräts mit dem Administrationsserver automatisch prüfen
Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk
Über das Überprüfen der Verbindungszeit des Geräts mit dem Administrationsserver
Client-Geräte auf dem Administrationsserver identifizieren
Verschieben von Geräten zu Administrationsgruppe
Den Administrationsserver für Client-Geräte ändern
Geräte, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind, auf einen anderen Administrationsserver verschieben
Server-Cluster und -Arrays
Client-Geräte von einem entfernten Standort einschalten, ausschalten und Neustart durchführen
Über die Verwendung einer dauerhaften Verbindung zwischen dem verwalteten Gerät und dem Administrationsserver
Über erzwungene Synchronisierung
Über den Zeitplan der Verbindung
Nachricht an Gerätenutzer senden
Arbeit mit dem Programm Kaspersky Security for Virtualization
Wechsel der Statuswerte von Geräten konfigurieren
Zuweisung von Tags an die Geräte die Anzeige der zugewiesenen Tags
Geräten automatisch Tags zuweisen
Anzeige und Einstellungen von Tags, die dem Gerät zugewiesen sind
Ferndiagnose der Client-Geräte. Kaspersky Security Center Ferndiagnosetool
Ferndiagnosetool mit dem Client-Gerät verbinden
Erzeugen einer Dump-Datei für eine Anwendung
Ablaufverfolgung aktivieren und deaktivieren, Protokolldatei downloaden
Anwendungseinstellungen herunterladen
Ereignisprotokolle downloaden
Herunterladen mehrerer Diagnoseinformationselemente
Diagnose starten und die Ergebnisse herunterladen
Starten, Beenden und Neustart von Programmen
UEFI-Schutzgeräte
Einstellungen eines verwalteten Geräts
Allgemeine Richtlinieneinstellungen
Richtlinieneinstellungen des Administrationsagenten
Benutzerkonten verwalten
Arbeiten mit Benutzerkonten
Benutzerkonto für einen internen Benutzer hinzufügen
Benutzerkonto eines internen Benutzers bearbeiten
Anzahl der zulässigen Eingabeversuche des Kennworts anpassen
Prüfung der Eindeutigkeit des Namens des internen Benutzers anpassen
Sicherheitsgruppen hinzufügen
Benutzer zur Gruppe hinzufügen

- Zugriffsrechte auf Anwendungsfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle
  - Zugriffsrechte auf Programmfunktionen
  - Vorkonfigurierte Benutzerrollen
  - Benutzerrollen hinzufügen
  - Einem Benutzer oder einer Sicherheitsgruppe eine Rolle zuweisen
  - Zuweisen von Berechtigungen an Benutzer und Gruppen
  - Ausdehnen von Benutzerrollen auf sekundäre Administrationsserver
- Benutzer zum Gerätebesitzer bestimmen
- Nachrichten an die Benutzer versenden
- Liste der mobilen Geräte des Benutzers anzeigen
- Benutzerzertifikat installieren
- Liste der für den Benutzer ausgestellten Zertifikate
- Über den Administrator des virtuellen Administrationsservers

Remote-Installation von Betriebssystemen und Programmen
- Betriebssystem-Abbilder erstellen
- Betriebssystem-Images installieren
- Adresse von KSN-Proxyserver anpassen
- Treiber für die Windows-Vorinstallationsumgebung (WinPE) hinzufügen
- Treiber zum Installationspaket mit dem Betriebssystem-Abbild hinzufügen
- Einstellungen des Tools sysprep.exe anpassen
- Bereitstellung von Betriebssystemen auf neuen Netzwerkgeräten
- Bereitstellung von Betriebssystemen auf Client-Geräten
- Installationspakete für Programme erstellen
- Ausgabe eines Zertifikats für Installationspakete von Programmen
- Programme auf Client-Geräten installieren

Umgang mit Objekt-Revisionen
- Über Objekt-Revisionen
- Anzeigen des Abschnitts "Revisionsverlauf"
- Vergleich der Revisionen des Objekts
- Einrichten der Speicherdauer für Revision des Objekts und für Information über gelöschte Objekte
- Anzeigen der Revision des Objekts
- Speichern der Revision des Objektes in einer Datei
- Rollback der Änderungen
- Hinzufügen einer Beschreibung der Revision

Objekte löschen
- Löschen eines Objekts
- Anzeigen von Informationen über gelöschte Objekte
- Dauerhaftes Löschen von Objekten aus der Liste der gelöschten Objekte

Verwaltung mobiler Geräte
- Szenario: Bereitstellung der Funktion "Verwaltung mobiler Geräte"
- Gruppenrichtlinie für die Verwaltung von iOS MDM-Geräten
- Aktivieren der Funktion "Verwaltung mobiler Geräte"
- Einstellungen der Komponente "Verwaltung mobiler Geräte" anpassen
- Komponente "Verwaltung mobiler Geräte" deaktivieren
- Arbeiten mit Befehlen für mobile Geräte
  - Befehle zur Verwaltung mobiler Geräte
  - Verwendung von Firebase Cloud Messaging

Befehle absenden
Status von Befehlen im Befehlsprotokoll anzeigen
Zertifikate für mobile Geräte verwenden
Starten des Assistenten für die Installation eines Zertifikats
Schritt 1. Auswählen des Zertifikattyps
Schritt 2. Auswählen des Gerätetyps
Schritt 3. Auswählen eines Benutzers
Schritt 4. Auswählen der Zertifikatquelle
Schritt 5. Zuweisen eines Tags zum Zertifikat
Schritt 6. Angeben der Veröffentlichungseinstellungen des Zertifikats
Schritt 7. Auswählen der Methode zur Benachrichtigung von Benutzers
Schritt 8. Generieren des Zertifikats
Regeln für das Ausstellen von Zertifikaten anpassen
Integration mit Public Key Infrastructure
Unterstützung von Kerberos Constrained Delegation aktivieren
Mobiles iOS-Gerät zur Liste der verwalteten Geräte hinzufügen
Mobiles Android-Gerät zur Liste der verwalteten Geräte hinzufügen
iOS MDM-Geräte verwalten
Ein iOS MDM-Profil mittels Zertifikat signieren
Konfigurationsprofil hinzufügen
Konfigurationsprofil auf dem Gerät hinzufügen
Konfigurationsprofil vom Gerät löschen
Hinzufügen eines neuen Geräts mittels der Veröffentlichung eines Links auf das Profil
Hinzufügen eines neuen Geräts mittels der Installation des Profils durch den Administrator
Provisioning-Profil hinzufügen
Provisioning-Profil auf dem Gerät installieren
Provisioning-Profil vom Gerät löschen
Verwaltete Apps hinzufügen
App auf dem mobilen Gerät installieren
App vom Gerät löschen
Roaming-Einstellungen auf einem mobilen iOS MDM-Gerät konfigurieren
Informationen über das iOS MDM-Gerät anzeigen
Ausschluss eines iOS MDM-Geräts von der Verwaltung
Senden von Befehlen an ein Gerät
Untersuchung des Ausführungsstatus der gesendeten Befehle
KES-Geräte verwalten
Paket mit mobilen Anwendungen für KES-Geräte erstellen
Zertifikatbasierte Authentifizierung von KES-Geräten aktivieren
Informationen über das KES-Gerät anzeigen
Ein KES-Gerät von der Verwaltung ausschließen
Verschlüsselung und Datenschutz
Liste der verschlüsselten Geräte anzeigen
Liste der Verschlüsselungsereignisse anzeigen
Liste der Verschlüsselungsereignisse in eine Textdatei exportieren
Verschlüsselungsberichte erstellen und anzeigen
Übertragung von Chiffrierschlüsseln zwischen Administrationsservern

- Datenverwaltung
  - Liste mit Objekten, die sich in der Datenverwaltung befinden, in eine Textdatei exportieren
  - Installationspakete
  - Grundlegende Statusvarianten der Dateien in der Datenverwaltung
  - Auslösen von Regeln im Smart Training-Modus
    - Liste der Funde anzeigen, die auf Regeln der Adaptiven Kontrolle von Anomalien beruhen
    - Ausschlüsse aus den Regeln zur Adaptiven Kontrolle von Anomalien hinzufügen
      - Schritt 1. Auswählen des Programms
      - Schritt 2. Auswählen der Richtlinie (Richtlinien)
      - Schritt 3. Verarbeiten der Richtlinie (Richtlinien)
  - Quarantäne und Backup
    - Aktivieren der Remote-Verwaltung von Dateien in der Datenverwaltung
    - Eigenschaften der Datei in der Datenverwaltung anzeigen
    - Dateien aus der Datenverwaltung entfernen
    - Dateien aus der Datenverwaltung wiederherstellen
    - Datei aus der Datenverwaltung auf der Festplatte speichern
    - Untersuchung der Dateien in Quarantäne
  - Aktive Bedrohungen
    - Unverarbeitete Dateien desinfizieren
    - Datei mit verschobener Verarbeitung auf Festplatte speichern
    - Datei aus dem Ordner "Aktive Bedrohungen" löschen
- Kaspersky Security Network (KSN)
  - Über KSN
  - Zugriff auf Kaspersky Security Network vorbereiten
  - KSN aktivieren und deaktivieren
  - Die akzeptierte KSN-Erklärung anzeigen
  - KSN Proxyserver-Statistik anzeigen
  - Eine aktualisierte KSN-Erklärung akzeptieren
  - Zusätzlicher Schutz durch Verwendung von Kaspersky Security Network
  - Feststellen, ob der Verteilungspunkt als KSN-Proxyserver fungiert
- Zwischen Online-Hilfe und Offline-Hilfe wechseln

Ereignisse in SIEM-Systeme exportieren

- Ereignisexport in SIEM-Systeme konfigurieren
- Vorläufige Bedingungen
- Über Ereignisse in Kaspersky Security Center
- Über den Ereignisexport
- Über das Konfigurieren des Ereignisexports in ein SIEM-System
- Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren
  - Ereignisse von Kaspersky-Anwendungen für den Export im Syslog-Format markieren
  - Allgemeine Ereignisse zum Export im Syslog-Format markieren
- Über das Exportieren von Ereignissen im Syslog-Format
- Über das Exportieren von Ereignissen mittels der Formate CEF und LEEF
- Konfiguration von Kaspersky Security Center für den Export an ein SIEM-System

Ereignisse direkt aus der Datenbank exportieren
Eine SQL-Abfrage mit dem Tool "klsql2" ausführen
Beispielhafte SQL-Abfrage, die mit dem Tool "klsql2" erstellt wurde
Anzeige des Namens der Datenbank von Kaspersky Security Center
Exportergebnisse anzeigen
Verwenden von SNMP zum Senden von Statistiken an Programme von Drittanbietern
Den SNMP-Dienst für die Verwendung mit Kaspersky Security Center konfigurieren
Kennungen des SNMP-Agenten und der SNMP-Objekte
Den Namen des Zeichenfolgenzählers aus einer Objektkennung ableiten
Werte von Objektkennungen für SNMP
Problemlösung
Arbeiten in einer Cloud-Umgebung
Über die Arbeit in der Cloud-Umgebung
Szenario: Bereitstellung für eine Cloud-Umgebung
Voraussetzungen für die Softwareverteilung von Kaspersky Security Center in einer Cloud-Umgebung
Hardwarevoraussetzungen des Administrationsservers in einer Cloud-Umgebung
Varianten der Lizenzierung in der Cloud-Umgebung
Datenbankoptionen zum Arbeiten in einer Cloud-Umgebung
Arbeit mit der Cloud-Umgebung Amazon Web Services
Über die Arbeit in der Cloud-Umgebung Amazon Web Services
Erstellen von IAM-Rollen und IAM-Benutzerkonten für Amazon EC2-Instances
Bereitstellung der Rechte für die Arbeit des Kaspersky Security Center Administrationsservers mit den AWS
IAM-Rolle für Administrationsserver erstellen
Erstellen eines IAM-Benutzerkontos für die Arbeit mit Kaspersky Security Center
Erstellen der IAM-Rolle für die Installation von Programmen auf Amazon EC2-Instances
Arbeiten mit Amazon RDS
Amazon RDS-Instance erstellen
Optionsgruppe für eine Amazon RDS-Instance erstellen
Ändern der Optionsgruppe
Ändern der Berechtigungen für die IAM-Rolle der Amazon RDS-DB-Instance
Amazon S3-Bucket für Datenbank vorbereiten
Datenbank auf Amazon RDS migrieren
Arbeiten mit der Cloud-Umgebung Microsoft Azure
Über das Arbeiten in Microsoft Azure
Erstellen eines Abonnements, einer Anwendungs-ID und eines Kennworts
Der Azure Anwendungs-ID eine Rolle zuweisen
Verteilen des Administrationsservers in Microsoft Azure und Auswählen der Datenbank
Mit Azure SQL arbeiten
Azure-Speicherkonto erstellen
Azure SQL-Datenbank und SQL Server erstellen
Datenbank auf Azure SQL migrieren
Arbeiten mit Google Cloud
Erstellen von Client-E-Mail, Projekt-ID und privatem Schlüssel
Arbeiten mit einer Instanz von Google Cloud SQL for MySQL
Erforderliche Komponenten für Client-Geräte in einer Cloud-Umgebung für die Arbeit mit Kaspersky Security Center
Erstellen von Installationspaketen, die zur Konfiguration der Cloud-Umgebung erforderlich sind

- Eine Cloud-Umgebung konfigurieren
  - Über den Assistenten zur Konfiguration der Cloud-Umgebung
  - Schritt 1. Auswählen der Methode zur Programmaktivierung
  - Schritt 2. Auswählen der Cloud-Umgebung
  - Schritt 3. Autorisieren in der Cloud-Umgebung
  - Schritt 4. Konfigurieren der Cloud-Synchronisation und Wählen weiterer Maßnahmen
  - Schritt 5. Konfigurieren von Kaspersky Security Network in der Cloud-Umgebung
  - Schritt 6. Konfigurieren von E-Mail-Benachrichtigungen in der Cloud-Umgebung
  - Schritt 7. Erstellen einer Erstkonfiguration des Schutzes für die Cloud-Umgebung
  - Schritt 8. Auswählen der auszuführenden Maßnahme, wenn das Betriebssystem während der Installation einen Neustart erfordert (für Cloud-Umgebung)
  - Schritt 9. Empfangen von Updates durch den Administrationsserver
- Überprüfen der Konfiguration
- Gruppe der Cloud-Geräte
- Abfrage des Netzwerksegments
  - Hinzufügen von Verbindungen für die Abfrage von Cloud-Segmenten
  - Entfernen von Verbindungen für die Abfrage von Cloud-Segmenten
  - Abfragezeitplan anpassen
- Installation von Programmen auf Geräten in einer Cloud-Umgebung
- Eigenschaften von Cloud-Geräten anzeigen
- Synchronisierung mit der Cloud
- Bereitstellung von Kaspersky Security Center in Yandex.Cloud

Appendix

- Zusatzoptionen
  - Automatisierung der Programmfunktion von Kaspersky Security Center. Tool klakaut
  - Arbeiten mit externen Instrumenten
  - "Laufwerk klonen"-Modus des Administrationsagenten
  - Vorbereiten eines Referenzgeräts mit installiertem Administrationsagenten, um ein Betriebssystemabbild zu erstellen
  - Einstellungen des Empfangs von Nachrichten von der Komponente "Überwachung der Dateiintegrität" anpassen
  - Wartung des Administrationsservers
  - Zugriff auf öffentliche DNS-Server
  - Fenster "Benachrichtigungsmethode"
  - Fenster Geräteauswahl
  - Fenster "Name des zu erstellenden Objekts festlegen"
- Besonderheiten der Verwaltungsoberfläche
  - Konsolenstruktur
  - Wie Daten im Arbeitsbereich aktualisiert werden
  - Wie in der Konsolenstruktur navigiert wird
  - Wie das Eigenschaftenfenster eines Objekts im Arbeitsbereich geöffnet wird
  - Wie eine Gruppe von Objekten im Arbeitsbereich ausgewählt wird
  - Wie die Auswahl von Spalten im Arbeitsbereich geändert wird
- Hilfe
  - Befehle des Kontextmenüs
  - Liste der verwalteten Geräte. Beschreibung von Spalten
  - Statusmeldungen der Geräte, Aufgaben und Richtlinien
  - Symbole der Status der Dateien in der Verwaltungskonsole

Suche und Export von Daten
Suche nach Geräten
Suchoptionen für Geräte
Masken in Zeichenfolgenvariablen verwenden
Reguläre Ausdrücke in der Suchzeile verwenden
Listen aus Dialogfenstern exportieren
Einstellungen für Aufgaben
Allgemeine Aufgabeneinstellungen
Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers
Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte
Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates
Erforderliche Updates installieren und Schwachstellen schließen
Globale Liste der Subnetze
Hinzufügen von Subnetzen zur globalen Liste der Subnetze
Anzeigen und Ändern von Subnetzeigenschaften in der globalen Liste der Subnetze
Administrationsagent für Windows, Linux und macOS: Vergleich
Kaspersky Security Center Web Console
Bereitstellungsdiagramm für Kaspersky Security Center Administrationsserver und Kaspersky Security Center Web Console
Von Kaspersky Security Center Web Console verwendete Ports
Benutzeroberfläche der Kaspersky Security Center Web Console
Abschnitte des Hauptmenüs anheften und lösen
Szenario: Installation und Erstkonfiguration von Kaspersky Security Center Web Console
Installation
Kaspersky Security Center installieren (Standardinstallation)
Kaspersky Security Center Web Console installieren
Installation der Kaspersky Security Center Web Console mit Verbindung zum Administrationsserver, der auf Knoten des Failover-Clusters installiert wurde
Kaspersky Security Center Web Console aktualisieren
Zertifikate für die Ausführung mit Kaspersky Security Center Web Console
Zertifikat für Kaspersky Security Center Web Console neu ausstellen
Zertifikat für Kaspersky Security Center Web Console ersetzen
Zertifikaten für vertrauenswürdige Administrationsserver in der Kaspersky Security Center Web Console angeben
Konvertieren eines pfx-Zertifikats in ein pem-Zertifikat
Migration von Kaspersky Security Center Windows
Migration nach Kaspersky Security Center Cloud Console
Migration nach Kaspersky Next XDR Expert
Migration nach Kaspersky Security Center Linux
Migration auf Kaspersky Security Center Linux mittels Daten-Backups des Administrationsservers
Migration zu Kaspersky Security Center Linux mittels Migrationsassistenten
Gruppenobjekte aus Kaspersky Security Center Windows exportieren
Importieren der Exportdatei in Kaspersky Security Center Linux
Verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen
In der Kaspersky Security Center Web Console anmelden und abmelden
Identitäts- und Zugriffsverwaltung in Kaspersky Security Center Web Console
Über die Identitäts- und Zugriffsverwaltung
Aktivieren der Identitäts- uns Zugriffsverwaltung: Szenario
Die Identitäts- und Zugriffsverwaltung in der Kaspersky Security Center Web Console konfigurieren

Die Kaspersky Industrial CyberSecurity for Networks in der Kaspersky Security Center Web Console registrieren
Token-Lebensdauer und Autorisierungs-Timeout der Identitäts- und Zugriffsverwaltung
IAM-Zertifikate herunterladen und verteilen
Die Identitäts- und Zugriffsverwaltung deaktivieren
Domänenauthentifizierung mithilfe der Protokolle NTLM und Kerberos konfigurieren
Administrationsserver konfigurieren
Verbindung zwischen Kaspersky Security Center Web Console und Administrationsserver anpassen
Protokollierung der Verbindungsereignisse des Administrationsservers konfigurieren
Die Internetzugriffseinstellungen für den Administrationsserver konfigurieren
Maximalen Anzahl an Ereignissen in der Ereignis-Datenverwaltung festlegen
Verbindungseinstellungen des Geräts mit Schutz auf UEFI-Ebene
Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen
Liste mit sekundären Administrationsservern anzeigen
Administrationsserver-Hierarchie löschen
Wartung des Administrationsservers
Schnittstelle konfigurieren
Virtuelle Administrationsserver verwalten
Einen virtuellen Administrationsserver erstellen
Einen virtuellen Administrationsserver aktivieren und deaktivieren
Einem virtuellen Administrationsserver einen Administrator zuweisen
Den Administrationsserver für Client-Geräte ändern
Einen virtuellen Administrationsserver löschen
Benutzerkonten-Schutz vor unbefugten Änderungen aktivieren
Daten des Administrationsservers sichern und wiederherstellen
Aufgabe zum Anlegen eines Backups
Administrationsserver auf anderes Gerät übertragen
Integrität der Module anhand der Tools klscmodchk und integrity_checker prüfen
Erstkonfiguration von Kaspersky Security Center Web Console
Schnellstartassistent (Kaspersky Security Center Web Console)
Schritt 1. Einstellungen für die Internetverbindung festlegen
Schritt 2. Erforderliche Updates herunterladen
Schritt 3. Zu sichernde Assets auswählen
Schritt 4. Verwendete Verschlüsselung für die Lösungen auswählen
Schritt 5. Plug-ins für verwaltete Programme konfigurieren
Schritt 6. Installieren der ausgewählten Plug-ins
Schritt 7. Herunterladen der Programmpakete Erstellen der Installationspakete
Schritt 8. Kaspersky Security Network konfigurieren
Schritt 9. Auswählen der Methode zur Programmaktivierung
Schritt 10. Festlegen der Einstellungen zur Verwaltung von Drittanbieter-Updates
Schritt 11. Erstellen einer grundlegenden Konfiguration für Netzwerkschutz
Schritt 12. Konfigurieren von E-Mail-Benachrichtigungen
Schritt 13. Durchführen einer Netzwerkabfrage
Schritt 14. Abschließen des Schnellstartassistenten
Verbinden mobiler Geräte
Szenario: Verbinden von mobilen Geräten mittels Verbindungs-Gateway
Szenario: Verbinden von mobilen Geräten mittels einem sekundären Administrationsserver in der DMZ
Über das Verbinden mobiler Geräte

Verbinden von externen Desktop-Geräten mit dem Administrationsserver
Über Verbindungsprofile für mobile Benutzer
Erstellen eines Verbindungsprofils für mobile Benutzer
Über das Umschalten eines Administrationsagenten auf einen anderen Administrationsserver
Erstellen der Regel für die Umstellung des Administrationsagenten gemäß dem Netzwerkspeicherort
Assistent für die Bereitstellung des Schutzes
Schritt 1. Assistent für die Bereitstellung des Schutzes starten
Schritt 2. Installationspaket auswählen
Schritt 3. Verteilungsmethode der Schlüsseldatei oder des Aktivierungscodes auswählen
Schritt 4. Auswählen der Version des Administrationsagenten
Schritt 5. Auswählen der Geräte
Schritt 6. Festlegen der Einstellungen für die Aufgabe zur Remote-Installation
Schritt 7. Verwaltung des Neustarts
Schritt 8. Deinstallieren inkompatibler Programme vor der Installation
Schritt 9. Verschieben von Geräten in die Gruppe "Verwaltete Geräte"
Schritt 10. Auswählen von Benutzerkonten für den Zugriff auf Geräten
Schritt 11. Beginnen der Installation
Bereitstellung der Kaspersky-Anwendungen über die Kaspersky Security Center Web Console
Szenario: Bereitstellung der Programme von Kaspersky über die Kaspersky Security Center Web Console
Beziehen von Plug-ins für Kaspersky-Anwendungen
Installationspakete für Kaspersky-Anwendungen herunterladen und erstellen
Größenbegrenzung für benutzerdefinierte Installationspakete anpassen
Programmpakete für Kaspersky-Anwendungen herunterladen
Die erfolgreiche Bereitstellung von Kaspersky Endpoint Security überprüfen
Autonome Installationspakete erstellen
Liste der autonomen Installationspakete anzeigen
Erstellen benutzerdefinierter Installationspakete
Installationspakete an sekundäre Administrationsserver verteilen
Anwendungen mit der Aufgabe zur Remote-Installation installieren
Eine Anwendung remote installieren
Programme mit Gruppenrichtlinien des Active Directory installieren
Anwendungen auf sekundären Administrationsservern installieren
Einstellungen für die Remote-Installation auf Unix-Geräten angeben
Kaspersky-Anwendungen starten und beenden
Verwaltung mobiler Geräte
Sicherheitsanwendungen von Drittanbietern ersetzen
Geräte im Netzwerk finden
Szenario: Netzwerkgeräte finden
Suchen von Geräten
Windows-Netzwerkabfrage
IP-Bereiche abfragen
IP-Bereich hinzufügen und bearbeiten
Zeroconf-Abfrage
Abfrage des Domänencontrollers
Authentifizierung und Verbindung mit einem Domänencontroller
Einen Samba-Domänencontroller konfigurieren
Aufbewahrungsregeln für nicht zugeordnete Geräte anpassen

Arbeitsgerätebestand
Informationen über neue Geräte hinzufügen
Kriterien zur Erkennung von Unternehmensgeräten anpassen
Kaspersky-Anwendungen: Lizenzierung und Aktivierung
Lizenzierung der verwalteten Programme
Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
Lizenzschlüssel des Administrationsservers hinzufügen
Lizenzschlüssel auf Client-Geräte verteilen
Lizenzschlüssel automatisch verteilen
Informationen zu verwendeten Lizenzschlüsseln anzeigen
Lizenzschlüssel aus der Datenverwaltung entfernen
Vereinbarung mit einem Endbenutzer-Lizenzvertrag widerrufen
Lizenzen für Kaspersky-Anwendungen verlängern
Kaspersky Marketplace zum Finden von Kaspersky-Unternehmenslösungen verwenden
Netzwerkschutz konfigurieren
Szenario: Netzwerkschutz konfigurieren
Geräteorientierte und benutzerorientierte Methode der Sicherheitsverwaltung
Richtlinien einrichten und verwalten: geräteorientierte Herangehensweise
Richtlinien einrichten und verwalten: benutzerorientierte Herangehensweise
Richtlinieneinstellungen des Administrationsagenten
Vergleich der Richtlinieneinstellungen des Administrationsagenten nach Betriebssystemen
Den ressourcenschonenden Modus des Administrationsagenten aktivieren und deaktivieren
Konfigurieren der Schutzeinstellungen für verwaltete Anwendungen
Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren
Anwendungen oder Software-Updates per Fernzugriff entfernen
Aufgaben
Über Aufgaben
Über den Gültigkeitsbereich von Aufgaben
Aufgaben erstellen
Aufgaben manuell starten
Aufgabenliste anzeigen
Allgemeine Aufgabeneinstellungen
Aufgaben exportieren
Aufgaben importieren
Assistent zum Ändern der Aufgabenkennwörter starten
Schritt 1. Anmeldedaten angeben
Schritt 2. Auszuführenden Vorgang auswählen
Schritt 3. Ergebnisse anzeigen
Aufgabe zur Remote-Ausführung von Skripten erstellen
Anwendungen mittels Aufgabe zur Remote-Ausführung von Skripten auf Geräten installieren
Benachrichtigungen und Überwachung für die Aufgabe zur Remote-Ausführung von Skripten konfigurieren
Archiv für die Aufgabe zur Remote-Ausführung von Skripten vorbereiten
Installationspaket auf Basis einer Manifestdatei erstellen
Client-Geräte verwalten
Einstellungen eines verwalteten Geräts
Administrationsgruppen anlegen
Geräte manuell zu einer Administrationsgruppe hinzufügen

- Manuelles Verschieben von Geräten oder Clustern in eine Administrationsgruppe
- Regeln für das Verschieben von Geräten erstellen
- Regeln für das Verschieben von Geräten kopieren
- Bedingungen für Verschiebungsregeln für Geräte
- Über Cluster und Server-Arrays
- Eigenschaften eines Cluster- oder Server-Arrays
- Maßnahmen anzeigen und konfigurieren, wenn Geräte als inaktiv angezeigt werden
- Über die Varianten für den Gerätestatus
- Wechsel der Statuswerte von Geräten konfigurieren
- Remotedesktopverbindung mit dem Client-Gerät herstellen
- Verbindung mit den Client-Geräten über die Windows Desktopfreigabe herstellen
- Geräteauswahlen
  - Geräteliste einer Geräteauswahl anzeigen
  - Geräteauswahl erstellen
  - Einstellungen einer Geräteauswahl anpassen
  - Geräteliste einer Geräteauswahl exportieren
  - Geräte in der Auswahl aus Administrationsgruppen löschen
- Geräte-Tags
  - Geräte-Tag erstellen
  - Geräte-Tag umbenennen
  - Geräte-Tag löschen
  - Geräte mit zugewiesenen Tags anzeigen
  - Tags anzeigen, die einem Gerät zugewiesen sind
  - Tags einem Gerät manuell zuweisen
  - Zugewiesene Tags von einem Gerät entfernen
  - Regeln für das automatische Zuweisen von Tags an Geräten anzeigen
  - Regeln für das automatische Zuweisen von Tags an Geräte bearbeiten
  - Regeln für das automatische Zuweisen von Tags an Geräte erstellen
  - Regeln für das automatische Zuweisen von Tags an Geräte ausführen
  - Regeln für das automatische Zuweisen von Tags an Geräte löschen
  - Verwalten von Geräte-Tags mit dem Tool klscflag

Richtlinien und Richtlinienprofile

- Über Richtlinien und Richtlinienprofile
- Über das Schloss und gesperrte Einstellungen
- Vererbung von Richtlinien und Richtlinienprofilen
  - Hierarchie der Richtlinien
  - Richtlinienprofile in einer Hierarchie von Richtlinien
  - Implementierung der Einstellungen auf einem verwalteten Gerät
- Richtlinien verwalten
  - Richtlinienliste anzeigen
  - Richtlinie erstellen
  - Richtlinie ändern
  - Allgemeine Richtlinieneinstellungen
  - Option zur Vererbung einer Richtlinie aktivieren und deaktivieren
  - Richtlinien kopieren
  - Richtlinie verschieben
  - Richtlinien exportieren

Richtlinien importieren
Diagramm für den Status der Richtlinienverteilung anzeigen
Richtlinien löschen
Richtlinienprofile verwalten
Profile einer Richtlinie anzeigen
Priorität eines Richtlinienprofils ändern
Richtlinienprofil erstellen
Richtlinienprofil ändern
Richtlinienprofil kopieren
Regeln für die Aktivierung des Richtlinienprofils erstellen
Richtlinienprofil löschen
Verschlüsselung und Datenschutz
Liste der verschlüsselten Laufwerke anzeigen
Liste der Verschlüsselungsereignisse anzeigen
Verschlüsselungsberichte erstellen und anzeigen
Zugriff auf ein verschlüsseltes Laufwerk im autonomen Modus gewähren
Benutzer und Benutzerrollen
Über Benutzerrollen
Benutzerkonten und Sitzungen anzeigen
Zugriffsrechte auf Anwendungsfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle
Zugriffsrechte auf Programmfunktionen
Vorkonfigurierte Benutzerrollen
Bestimmten Objekten Zugriffsrechte zuweisen
Zugriffsrechte an Benutzer und Sicherheitsgruppen zuweisen
Benutzerkonto für einen internen Benutzer hinzufügen
Eine Sicherheitsgruppe erstellen
Benutzerkonto eines internen Benutzers bearbeiten
Eine Sicherheitsgruppe bearbeiten
Einem Benutzer oder einer Sicherheitsgruppe eine Rolle zuweisen
Benutzerkonten zu einer internen Sicherheitsgruppe hinzufügen
Benutzer zu Gerätebesitzern ernennen
Konfigurieren der zweistufigen Überprüfung für alle Benutzer
Über die zweistufige Überprüfung
Die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren (Web Console)
Zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren (MMC-basiert)
Obligatorische zweistufige Überprüfung für alle Benutzer aktivieren (Web Console)
Zweistufige Überprüfung für alle Benutzer aktivieren (MMC-basiert)
Zweistufige Überprüfung für ein Benutzerkonto deaktivieren (Web Console)
Zweistufige Überprüfung für ein Benutzerkonto deaktivieren (MMC-basiert)
Obligatorische zweistufige Überprüfung für alle Benutzer deaktivieren (Web Console)
Obligatorische zweistufige Überprüfung für alle Benutzer deaktivieren (MMC-basiert)
Benutzerkonten von der zweistufigen Überprüfung ausschließen (Web Console)
Benutzerkonten von der zweistufigen Überprüfung ausschließen (MMC-basiert)
Den Namen eines Sicherheitscode-Ausstellers bearbeiten (Web Console)
Name eines Sicherheitscode-Ausstellers bearbeiten (MMC-basiert)
Die zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren (Web Console)
Zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren (MMC-basiert)

Neuen geheimen Schlüssel generieren
Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten
Benutzer nach der Installation des Administrationsagenten zum Linux-Gerätebesitzer ernennen
Löschen eines Benutzers oder einer Sicherheitsgruppe
Kennwort eines Benutzerkontos ändern
Benutzerrollen erstellen
Benutzerrollen bearbeiten
Gültigkeitsbereich einer Benutzerrolle bearbeiten
Benutzerrollen löschen
Richtlinienprofile mit Rollen verbinden
Ausdehnen von Benutzerrollen auf sekundäre Administrationsserver
Kennwort des Benutzerkontos ändern
Lokale Administratorrechte entziehen
Umgang mit Objekt-Revisionen
Objekte auf eine frühere Version zurück rollen
Hinzufügen einer Beschreibung der Revision
Revision einer Richtlinie anzeigen und speichern
Objekte löschen
Kaspersky Security Network (KSN)
Über KSN
Zugriff auf KSN einrichten
Verwendung von KSN aktivieren und deaktivieren
Die akzeptierte KSN-Erklärung anzeigen
Eine aktualisierte KSN-Erklärung akzeptieren
Feststellen, ob der Verteilungspunkt als KSN-Proxyserver fungiert
Szenario: Upgrades von Kaspersky Security Center und der verwalteten Sicherheitsanwendungen
Datenbanken und Anwendungen von Kaspersky aktualisieren
Szenario: Datenbanken und Programme von Kaspersky regelmäßig aktualisieren
Über das Aktualisieren der Datenbanken, Software-Module und Programme von Kaspersky
Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen
Heruntergeladene Updates prüfen
Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen
Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren
Automatische Installation von Updates für Kaspersky Endpoint Security für Windows
Programm-Updates genehmigen und ablehnen
Aktualisieren des Administrationsservers
Autonomes Modell für den Download von Updates aktivieren und deaktivieren
Datenbanken und Software-Module von Kaspersky auf autonomen Geräten aktualisieren
Web-Plugins sichern und wiederherstellen
Verteilungspunkte und Verbindungs-Gateways anpassen
Typische Konfiguration von Verteilungspunkten: Einzelbüro
Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros
Über das Zuweisen von Verteilungspunkten
Verteilungspunkte automatisch zuweisen
Verteilungspunkte manuell zuweisen
Liste mit Verteilungspunkten für eine Administrationsgruppe bearbeiten

Erzwungene Synchronisierung
Push-Server aktivieren
Drittanbieter-Programme auf Client-Geräten verwalten
Updates für Drittanbieter-Programme installieren
Szenario: Aktualisieren von Software von Drittanbietern
Updates für Drittanbieter-Programme installieren
Erstellen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"
Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates
Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen
Regeln für die Update-Installation hinzufügen
Erstellen der Aufgabe "Windows-Updates installieren"
Informationen zu verfügbaren Updates für Drittanbieter-Programme anzeigen
Liste der verfügbaren Software-Updates in eine Datei exportieren
Genehmigen und Ablehnen der Updates für Drittanbieter-Programme
Erstellen der Aufgabe "Windows-Updates synchronisieren"
Drittanbieter-Anwendungen automatisch aktualisieren
Schwachstellen in Drittanbieter-Anwendungen schließen
Szenario: Finden und Schließen von Schwachstellen in Programmen von Drittanbietern
Über die Suche nach und das Schließen von Software-Schwachstellen
Schwachstellen in Drittanbieter-Anwendungen schließen
Erstellen der Aufgabe "Schwachstellen schließen"
Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen
Regeln für die Update-Installation hinzufügen
Auswählen von Benutzerkorrekturen für Schwachstellen in Programmen von Drittanbietern
Anzeigen von Informationen zu Schwachstellen in Programmen, die auf allen verwalteten Geräten erkannt wurden
Anzeigen von Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden
Statistik über Schwachstellen auf verwalteten Geräten anzeigen
Exportieren der Liste von Schwachstellen in Programmen in eine Datei
Ignorieren von Schwachstellen in Programmen
Verwalten des Programmstarts auf Client-Geräten
Programmkontrolle zur Verwaltung ausführbarer Dateien verwenden
Modi und Kategorien der Programmkontrolle
Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen
Erstellen einer manuell zu erweiternden Programmkategorie
Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen
Erstellen einer Programmkategorie mit ausführbaren Dateien aus einem ausgewählten Ordner
Liste der Programmkategorien anzeigen
Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen
Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows konfigurieren
Liste der auf Client-Geräten installierten Anwendungen abrufen und anzeigen
Installationspaket eines Drittanbieter-Programms aus der Kaspersky-Datenbank erstellen
Einstellungen des Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank anzeigen und anpassen
Einstellungen des Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank
Anwendungs-Tags
Anwendungs-Tag erstellen
Anwendungs-Tag umbenennen

Einer Anwendung Tags zuweisen
Zugewiesene Tags von einer Anwendung entfernen
Anwendungs-Tag löschen
Überwachung und Berichterstattung
Szenario: Überwachung und Berichterstattung
Über die Arten der Überwachung und Berichterstattung
Dashboard und Widgets
Dashboard verwenden
Dem Dashboard Widgets hinzufügen
Widgets im Dashboard verbergen
Widgets auf dem Dashboard verschieben
Größe oder Darstellung von Widgets ändern
Einstellungen von Widgets ändern
Über den Nur-Dashboard-Modus
Nur-Dashboard-Modus konfigurieren
Verwaltungs- und Schutzberichte
Berichte verwenden
Berichtsvorlage erstellen
Eigenschaften von Berichtsvorlagen anzeigen und bearbeiten
Einen Bericht in eine Datei exportieren
Bericht erstellen und anzeigen
Aufgabe zum Berichtsversand anlegen
Berichtsvorlagen löschen
Ereignisse und Ereignisauswahl
Über Kaspersky Security Center
Ereignisauswahlen verwenden
Ereignisauswahl erstellen
Ereignisauswahl bearbeiten
Liste mit einer Ereignisauswahl anzeigen
Ereignisauswahl exportieren
Ereignisauswahl importieren
Informationen zu einem Ereignis anzeigen
Ereignisse in eine Datei exportieren
Verlauf eines Objekts aus einem Ereignis heraus anzeigen
Ereignisse löschen
Ereignisauswahl löschen
Speicherdauer für ein Ereignis festlegen
Ereignisse der Komponenten von Kaspersky Security Center
Datenstruktur der Beschreibungen von Ereignistypen
Ereignisse des Administrationsservers
Ereignisse des Administrationsservers: Kritisch
Ereignisse des Administrationsservers: Funktionsfehler
Ereignisse des Administrationsservers: Warnung
Ereignisse des Administrationsservers: Information

Ereignisse des Administrationsagenten
Administrationsagent: Ereignisse bei Funktionsfehlern
Ereignisse des Administrationsagenten: Warnung
Ereignisse des Administrationsagenten: Information
Ereignisse des iOS MDM-Servers
Ereignisse des iOS MDM-Servers: Funktionsfehler
Ereignisse des iOS MDM-Servers: Warnung
Ereignisse des iOS MDM-Servers: Information
Häufige auftretende Ereignisse blockieren
Über das Blockieren von häufig auftretenden Ereignissen
Das Blockieren häufig auftretender Ereignissen verwalten
Die Blockade häufig auftretender Ereignisse aufheben
Benachrichtigungen und Gerätestatus
Benachrichtigungen verwenden
Bildschirmbenachrichtigungen anzeigen
Über die Varianten für den Gerätestatus
Wechsel der Statuswerte von Geräten konfigurieren
Einstellungen für das Versenden von Benachrichtigungen anpassen
Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei
Kaspersky-Mitteilungen
Über Kaspersky-Mitteilungen
Einstellungen für die Kaspersky-Mitteilungen festlegen
Kaspersky-Mitteilungen deaktivieren
Informationen über die Erkennung von Bedrohungen anzeigen
Cloud Discovery
Cloud Discovery über das Widget aktivieren
Cloud Discovery-Widget zum Dashboard hinzufügen
Informationen über die Verwendung von Cloud-Diensten anzeigen
Risikostufe eines Cloud-Dienstes
Zugriffs auf unerwünschte Cloud-Dienste blockieren
Protokollieren der Aktivitäten der Kaspersky Security Center Web Console
Integration von Kaspersky Security Center und weiteren Lösungen
Hintergrundverbindung herstellen
Ereignisse in SIEM-Systeme exportieren
Ereignisexport in SIEM-Systeme konfigurieren
Vorläufige Bedingungen
Über Ereignisse in Kaspersky Security Center
Über den Ereignisexport
Über das Konfigurieren des Ereignisexports in ein SIEM-System
Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren
Über das Markieren von Ereignissen zum Export in SIEM-Systeme im Syslog-Format
Ereignisse von Kaspersky-Anwendungen zum Export im Syslog-Format markieren
Allgemeine Ereignisse zum Export im Syslog-Format markieren
Über das Exportieren von Ereignissen mittels der Formate CEF und LEEF
Ereignisse in das CEF- oder LEEF-Format konvertieren
Über das Exportieren von Ereignissen im Syslog-Format
Konfiguration von Kaspersky Security Center für den Export an ein SIEM-System

Ereignisse direkt aus der Datenbank exportieren
Eine SQL-Abfrage mit dem Tool "klsql2" ausführen
Beispielhafte SQL-Abfrage, die mit dem Tool "klsql2" erstellt wurde
Anzeige des Namens der Datenbank von Kaspersky Security Center
Exportergebnisse anzeigen
Arbeiten mit Kaspersky Security Center Web Console in einer Cloud-Umgebung
Konfiguration der Cloud-Umgebung in Kaspersky Security Center Web Console
Schritt 1. Überprüfen der erforderlichen Plug-ins und Installationspakete
Schritt 2. Lizenzieren des Programms
Schritt 3. Auswählen der Cloud-Umgebung und Autorisierung
Schritt 4. Abfragen des Segments, Konfigurieren der Cloud-Synchronisation und Wählen weiterer Maßnahmen
Schritt 5. Auswählen der Anwendung, für die eine Richtlinie und Aufgaben erstellt werden sollen
Schritt 6. Konfiguration von Kaspersky Security Network für Kaspersky Security Center
Schritt 7. Erstellen einer Erstkonfiguration des Schutzes
Abfrage von Netzwerksegmenten mittels Kaspersky Security Center Web Console
Hinzufügen von Verbindungen für die Abfrage von Cloud-Segmenten
Entfernen einer Verbindung für die Abfrage von Cloud-Segmenten
Konfiguration des Abfragezeitplans durch Kaspersky Security Center Web Console anpassen
Anzeigen der Ergebnisse der Abfrage des Cloud-Segments durch Kaspersky Security Center Web Console
Anzeigen der Eigenschaften von Cloud-Geräten durch Kaspersky Security Center Web Console
Synchronisation mit der Cloud: Konfigurieren der Verschiebungsregel
Remote-Installation von Programmen auf virtuellen Maschinen von Azure
Erstellen der Aufgabe zum Backup der Daten des Administrationsservers unter Verwendung eines Cloud-DBMS
Ferndiagnose der Client-Geräte
Öffnen des Fensters für die Ferndiagnose
Aktivieren und Deaktivieren der Ablaufverfolgung für Programme
Herunterladen der Protokolldateien eines Programms
Löschen der Protokolldateien
Anwendungseinstellungen herunterladen
Ereignisprotokolle downloaden
Starten, Stoppen und Neustarten der Anwendung
Remote-Diagnose für den Kaspersky Security Center Administrationsagenten ausführen und Ergebnisse herunterladen
Ausführen eines Programms auf einem Client-Gerät
Erzeugen einer Dump-Datei für eine Anwendung
Ferndiagnose auf einem Linux-basierten Client-Gerät ausführen
Dateien aus Quarantäne und Backup herunterladen und löschen
Dateien aus Quarantäne und Backup herunterladen
Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console ändern
API-Referenzhandbuch
Bewährte Verfahren für Dienstanbieter
Planung der Bereitstellung für Kaspersky Security Center
Internetzugriff für den Administrationsserver bereitstellen
Typische Konfiguration von Kaspersky Security Center
Über Verteilungspunkte
Hierarchie des Administrationsservers
Virtuelle Administrationsserver
Mobile Geräte mit installiertem Kaspersky Endpoint Security für Android verwalten

Bereitstellung und Erstkonfiguration
Installationsempfehlungen für den Administrationsserver
Benutzerkonten für die Dienste des Administrationsservers auf dem Failover-Cluster erstellen
Auswahl des DBMS
Adresse des Administrationsservers angeben
Schutz im Netzwerk eines Kundenunternehmens anpassen
Richtlinie für Kaspersky Endpoint Security manuell konfigurieren
Einstellungen der Richtlinie im Abschnitt "Erweiterter Schutz"
Einstellungen der Richtlinie im Abschnitt "Basisschutz"
Einstellungen der Richtlinie im Abschnitt "Allgemeine Einstellungen"
Einstellungen der Richtlinie im Abschnitt "Konfiguration von Ereignissen"
Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren
Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security
Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen
Manuelle Konfiguration der Gruppenaufgabe zur Installation von Updates und zum Schließen von Schwachstellen
Aufbau der Struktur von Administrationsgruppen und Zuweisung von Verteilungspunkten
Typische Konfiguration des MSP-Kunden: Einzelbüro
Typische Konfiguration des MSP-Kunden: Mehrere kleine, eigenständige Büros
Richtlinienhierarchie, Verwendung von Richtlinienprofilen
Hierarchie der Richtlinien
Richtlinienprofile
Aufgaben
Verschiebungsregeln für Geräte
Software-Kategorisierung
Mandantenfähige Programme
Verschieben ins Backup und Wiederherstellen der Einstellungen des Administrationsservers
Ein Gerät mit dem Administrationsserver ist ausgefallen
Die Einstellungen des Administrationsservers oder der Datenbank sind beschädigt
Softwareverteilung für den Administrationsagenten und die Sicherheitsanwendung
Erstmalige Bereitstellung
Anpassen der Einstellungen der Installer
Installationspakete
Eigenschaften des MSI-Installers und der Transformationsdateien
Bereitstellung mithilfe von Drittanbieter-Tools zur Remote-Installation von Apps
Allgemeinen Angaben über die Aufgaben zur Remote-Installation der Apps von Kaspersky Security Center
Bereitstellung mithilfe des Mechanismus der Gruppenrichtlinien von Microsoft Windows
Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center
Start der von Kaspersky Security Center gebildeten autonomen Pakete
Funktion zur manuellen Installation von Apps
Remote-Installation von Apps auf Geräte mit installiertem Administrationsagenten
Verwaltung des Neustarts von Geräten in der Aufgabe zur Remote-Installation
Zweckdienlichkeit des Datenbanken-Updates im Installationspaket der Antiviren-App
Entfernen der inkompatiblen Sicherheitsanwendungen von Drittanbietern
Einen kennwortgeschützten Administrationsagenten über die Eingabeaufforderung entfernen
Verwendung von Tools zur Remote-Installation der Apps von Kaspersky Security Center für den Start von beliebigen ausführbaren Dateien auf den verwalteten Geräten
Monitoring der Bereitstellung

Anpassen der Einstellungen der Installer
Allgemeine Informationen
Installation im Silent-Modus (mit Antwortdatei)
Installation des Administrationsagenten im Silent-Modus (ohne Antwortdatei)
Teilweises Anpassen der Installationseinstellungen durch setup.exe
Installationseinstellungen für den Administrationsserver
Installationseinstellungen des Administrationsagenten
Virtuelle Infrastruktur
Empfehlungen zur Senkung der Belastung auf den virtuellen Maschinen
Unterstützung von dynamischen virtuellen Maschinen
Unterstützung des Kopierens von virtuellen Maschinen
Unterstützung des Rollbacks des Dateisystems für Geräte mit Administrationsagent
Über Verbindungsprofile für mobile Benutzer
Bereitstellung der Funktionalität "Verwaltung mobiler Geräte"
Verbindung von KES-Geräten mit dem Administrationsserver
Direkte Verbindung der Geräte mit dem Administrationsserver
Anschlussschema für KES-Geräte mit dem Server unter Verwendung der erzwungenen Delegierung Kerberos (KCD)
Verwendung von Firebase Cloud Messaging
Integration in die Public-Key-Infrastruktur
Kaspersky Security Center Webserver
Weitere Routinearbeiten
Farbliche Kennzeichnungen und protokollierte Ereignissen in der Verwaltungskonsole überwachen
Remote-Zugriff auf verwaltete Geräte
Verwenden der Option "Verbindung mit Administrationsserver nicht trennen" zur Bereitstellung einer dauerhaften Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver
Über das Überprüfen der Verbindungszeit des Geräts mit dem Administrationsserver
Über erzwungene Synchronisierung
Über das Tunneln von Verbindungen
Handbuch zur Skalierung
Zu diesem Handbuch
Informationen zu Einschränkungen von Kaspersky Security Center
Berechnungen für die Administrationsserver
Berechnung von Hardwareressourcen für den Administrationsserver
Hardwarevoraussetzungen für DBMS und Administrationsserver
Berechnung des Speicherplatzes in der Datenbank
Berechnung des Speicherplatzes auf dem Laufwerk (mit und ohne Berücksichtigung der Verwendung von Schwachstellen- und Patch-Management)
Berechnung der Anzahl und der Konfiguration der Administrationsserver
Empfehlungen für die Verbindung dynamischer virtueller Maschinen mit Kaspersky Security Center
Berechnungen für Verteilungspunkte und Verbindungs-Gateways
Voraussetzungen für Verteilungspunkte
Anzahl und Konfiguration der Verteilungspunkte bestimmen
Berechnung der Anzahl der Verbindungs-Gateways
Speicherung der Daten zu Ereignissen für Aufgaben und Richtlinien
Besonderheiten und optimale Einstellungen bestimmter Aufgaben
Häufigkeit der Gerätesuche
Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers und zur Wartung des Administrationsservers

Gruppenaufgaben zum Update von Kaspersky Endpoint Security
Inventarisierungsaufgabe
Informationen zur Netzwerkauslastung zwischen dem Administrationsserver und den geschützten Geräten
Verbrauch von Datenverkehr bei der Ausführung verschiedener Szenarien
Mittleren Verbrauch von Datenverkehr in 24 Stunden
Anfrage an den Technischen Support
Technischen Support erhalten
Technischer Support mit Kaspersky CompanyAccount
Dump-Dateien des Administrationsservers abrufen
Informationsquellen über das Programm
Glossar
Administrationsagent
Administrationsgruppe
Administrationsserver
Administrationsserver-Client (Client-Gerät)
Administrator des Anbieters
Administrator von Kaspersky Security Center
Administrator-Arbeitsplatz
Administratorberechtigungen
Aktiver Schlüssel
Amazon EC2-Instance
Amazon Machine Image (AMI)
Anbieter von Antiviren-Schutz
Antiviren-Datenbanken
App Store
Aufgabe
Aufgabe für eine Reihe von Geräten
Aufgabeneinstellungen
Authentifizierungsagent
AWS Application Program Interface (AWS API)
AWS IAM-Zugriffsschlüssel
AWS-Managementkonsole
Backup-Ordner
Broadcast-Domäne
Client-Administrator
Cloud Discovery
Cloud-Umgebung
Daten-Backup des Administrationsservers
Demilitarisierte Zone (DMZ)
Direkte Anwendungsverwaltung
Ereignis-Datenverwaltung
Ereigniskategorie des Patches
Erzwungene Installation
Gerät mit Schutz auf UEFI-Ebene
Gerätebesitzer
Geteiltes Zertifikat
Grenzwert für Virenaktivität

Gruppenaufgabe
Gültigkeitsdauer der Lizenz
Härtungsleitfaden
Home-Administrationsserver
HTTPS
IAM-Benutzer
IAM-Rolle
Identitäts- und Zugriffsverwaltung (IAM)
Inkompatibles Programm
Installationspaket
Interne Benutzer
iOS MDM-Gerät
iOS MDM-Profil
iOS MDM-Server
JavaScript
Kaspersky Private Security Network (KPSN)
Kaspersky Security Center Operator
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center Webserver
Kaspersky Security Network (KSN)
Kaspersky-Update-Server
KES-Gerät
Konfigurationsprofil
Lightweight Nagent (LWNGT)
Lizenzierte Anwendungsgruppe
Lokale Aufgabe
Lokale Installation
Manuelle Installation
MITM-Angriff
Network Location Awareness (NLA)
Netzwerk-Antiviren-Schutz
Netzwerk-Schutzstatus
Programmeinstellungen
Provisioning-Profil
Remote-Installation
Richtlinie
Schlüsseldatei
Schutzstatus
Schwachstelle
Server für mobile Geräte
Signifikanz des Ereignisses
SSL
Update
Upgraden von Kaspersky Security Center (Aktualisieren)
Verbindungs-Gateway
Verfügbares Update
Verteilungspunkt

Verwaltete Geräte
Verwaltungs-Plug-in
Verwaltungskonsole
Virenangriff
Virtueller Administrationsserver
Wiederherstellung
Wiederherstellung der Daten des Administrationsservers
Windows Server Update-Dienst (WSUS)
Zentralisierte Anwendungsverwaltung
Zertifikat des Administrationsservers
Zusätzlicher Lizenzschlüssel (oder Reserve-Lizenzschlüssel)
Informationen über den Code von Drittherstellern
Markenrechtliche Hinweise
Bekannte Probleme

Kaspersky Security Center 15.1 Hilfe

	**Neuerungen** Erfahren Sie, was in der aktuellsten Version der Anwendung neu ist.		**Netzwerkschutz konfigurieren** Verwalten Sie die Sicherheit der Organisation.
	**Hard- und Softwarevoraussetzungen** Überprüfen Sie, welche Betriebssysteme und Anwendungsversionen unterstützt werden.		**Kaspersky-Programme. Datenbanken-Update und Update der Programm-Module** Sorgen Sie für die ununterbrochene Zuverlässigkeit des Schutzsystems.
	**Softwareverteilung und Erstkonfiguration** Planen Sie die Verwendung von Ressourcen, installieren Sie den Administrationsserver, installieren Sie den Administrationsagenten und die Sicherheitsanwendungen auf Client-Geräten und konsolidieren Sie die Geräte in Administrationsgruppen.		**Überwachung und Berichterstattung** Zeigen Sie Ihre Infrastruktur, den Schutzstatus und Statistiken an. Verwalten Sie den Zugriff auf Cloud-Dienste mit Cloud Discovery.
	**Geräte im Netzwerk finden** Finden Sie vorhandene und neue Geräte im Netzwerk Ihres Unternehmens.		**Ersetzen von Sicherheitsanwendungen von Drittanbietern** Lernen Sie Methoden zum Deinstallieren von inkompatiblen Anwendungen.
	**Kaspersky-Programme. Zentralisierte Bereitstellung** Bereitstellung der Kaspersky-Anwendungen.		**Verteilungspunkte und Verbindungs-Gateways anpassen** Konfigurieren Sie die Verteilungspunkte.
	**Update der vorherigen Version von Kaspersky Security Center** Aktualisieren Sie von einer Vorgängerversion auf Kaspersky Security Center 15.1.		**Bewährte Verfahren für Dienstanbieter (nur Online-Hilfe)** Erfahren Sie mehr über die Softwareverteilung, Einstellungen und Nutzung des Programms, sowie über Möglichkeiten zur Lösung von typischen Problemen, die bei der Ausführung des Programms entstehen.
	**Kaspersky-Programme. Lizenzverwaltung und Aktivierung** Aktivieren Sie die Kaspersky-Anwendungen mit wenigen Schritten.		**Handbuch zur Skalierung (nur Online-Hilfe)** Berücksichtigen Sie für eine optimale Leistung unter verschiedenen Arbeitsbedingungen die Anzahl der Geräte im Netzwerk, die Netztopologie und den erforderlichen Funktionsumfang von Kaspersky Security Center.
	**Ereignisse in SIEM-Systeme exportieren** Konfigurieren Sie den Export von Ereignissen in SIEM-Systeme zur Analyse.		**Schwachstellen- und Patch-Management** Schwachstellen in Drittanbieter-Programmen finden und schließen.
	**Arbeiten in einer Cloud-Umgebung** Stellen Sie Kaspersky Security Center in Cloud-Umgebungen bereit: Amazon Web Services™, Microsoft Azure™ und Google™ Cloud Platform.		**Häufig gestellte Fragen (nur Englisch)** Hier finden Sie Anweisungen zur Lösung häufiger Probleme.
	**Schnellstartanleitung für Kaspersky Endpoint Security for Business** Erste Schritte mit Kaspersky Endpoint Security for Business: Installation und Konfiguration der Lösung. Sie können sich auch den Funktionsvergleich von Kaspersky Security Center ansehen, um die am besten geeignete Methode zur Verwaltung der Netzwerksicherheit auszuwählen.		

Neuerungen

Kaspersky Security Center 15.1 – Update 2

Das Kaspersky Security Center 15.1 Update 2 behebt Probleme, die von Benutzern und dem Testteam gemeldet wurden:

- Aufgaben für einen Gültigkeitsbereich von Linux-Geräten, der durch den Import einer txt-Datei angegebene wurde, werden jetzt korrekt ausgeführt.
- Bei der Installation einer Kaspersky-Anwendung mithilfe einer Aufgabe zur Remote-Installation, die auf einem virtuellen Administrationsserver erstellt wurde, werden jetzt die Installationspakete nur über den Verteilungspunkt, der von diesem virtuellen Administrationsserver verwaltet wird, mithilfe von Betriebssystem-Tools auf die verwalteten Geräte übertragen.
- Es wurde ein Problem behoben, durch das sich ein sekundärer Administrationsserver nach der Rotation des Zertifikats des sekundären Servers nicht wieder mit dem primären Administrationsserver verbinden konnte.
- Es wurden Probleme mit TLS-Verbindungen behoben.
- Es wurde ein Problem behoben, das während der Benutzeranmeldung zu mehreren Fehlern vom Typ "Ungültiger Typumwandlung" führte.
- Kaspersky Security Center versendet jetzt Ereignisbenachrichtigungen korrekt per E-Mail.
- Es wurde ein Problem beim Hinzufügen des Ordners *Updates* zur Backup-Kopie behoben, wenn Kaspersky Security Center von Version 14.2 auf Version 15.1 aktualisiert wurde.
- Das Ablaufdatum der Lizenzierung für eine Kaspersky-Anwendung wird jetzt in der Kaspersky Security Center Web Console korrekt angezeigt.
- Die Befehle **Mobiles Gerät orten** und **Standortverlauf des Geräts abrufen** werden jetzt ordnungsgemäß ausgeführt.
- Es wurde ein Problem behoben, durch das Installationspakete mit Zertifikaten für Mobilgeräte 1 Stunde nach dem Download oder 24 Stunden ohne Verwendung nicht automatisch gelöscht wurden.
- Ein durch ein bestimmtes Tag aktiviertes Richtlinienprofil wird jetzt korrekt auf die Geräte angewendet, deren Beschreibungen dieses Tag enthalten.
- Es wurde ein Problem behoben, das dazu führte, dass im Ereignisprotokoll Fehlermeldungen der PostgreSQL-Datenbank angezeigt wurden.
- Das Ausschließen eines Kontos von der zweistufigen Überprüfung funktioniert jetzt korrekt.
- Es wurde ein Problem behoben, durch das die Abmeldung von der Kaspersky Security Center Web Console nicht ordnungsgemäß funktionierte, wenn die Domänenauthentifizierung mit aktivierter Identitäts- und Zugriffsverwaltung verwendet wurde.
- Beim Aktualisieren eines Web-Plug-ins zur Verwaltung wird jetzt durch Anklicken des Links für die gewünschte Version der Download gestartet.

- Behobene Probleme in Berichten:
  - Wenn Sie für den Bericht über Bedrohungen und den Update-Bericht eine Aufgabe zur Zustellung erstellen und den Zeitplan auf **Monatlich** festlegen, werden die Berichte jetzt korrekt mit Daten befüllt.
  - In der Vorlage für den *Bericht über den Status der Programmkomponenten* werden die Filter nach dem Komponentennamen korrekt angewendet.
  - Der *Bericht über die Bereitstellung des Schutzes* kann jetzt so gefiltert werden, dass nur die Geräte angezeigt werden, auf denen keine Kaspersky-Anwendungen installiert sind. Dies hilft beim Erkennen der Geräte, auf denen die Anwendungen installiert werden sollen.
- Das Widget **Cloud Discovery** wird unabhängig davon, ob Sie über die Berechtigung **Ausführen** im Bereich **Allgemeine Funktionen: Grundlegende Funktionen** verfügen oder nicht, korrekt angezeigt.
- Verbesserte Leistung von gespeicherten Prozeduren und Datenbankvorgängen.
- Es wurde ein Problem behoben, durch das abgelaufene Zertifikate, die mit nicht existierenden Benutzern verknüpft waren, dazu führten, dass der Erneuerungsprozess für alle Benutzer angehalten wurde.
- Es wurden Probleme mit der korrekten Handhabung von Zertifikaten behoben.
- Nach dem Update von Kaspersky Security Center Version 14.2 auf Version 15.1 werden jetzt autonome Installationspakete korrekt vom sekundären Administrationsserver in die Verwaltungskonsole heruntergeladen.
- Es wurde ein Fehler behoben, bei dem durch das Aktivieren der Verwendung von Kaspersky Security Network (KSN) in der Kaspersky Security Center Web Console innerhalb der Richtlinie einer Kaspersky-Anwendung, die KSN-Erklärung in den folgenden Anwendungsversionen nicht akzeptiert werden konnte: Kaspersky Endpoint Security für Linux Version 12.2 oder früher, Kaspersky Industrial CyberSecurity for Linux Nodes Version 1.5 oder früher, Kaspersky Security for Virtualization Light Agent Version 6.0 und 6.1, Kaspersky Embedded Systems Security for Linux Version 3.3 sowie Kaspersky Security für Windows Server Version 11.0.1.897.
- Es wurde ein Problem behoben, durch das ein Richtlinienprofil nicht auf Linux-basierte Geräte angewendet wurde, die zu einer Active Directory-Domänengruppe gehörten.
- Es wurde ein Problem behoben, das bei Verbindungsversuchen von mehreren sekundären Administrationsservern der zweiten Ebene zum primären Administrationsserver auftrat.

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 enthält eine Reihe neuer Funktionen und Verbesserungen:

- Cloud Discovery. Mit dieser neuen Funktion können Sie Versuche überwachen, Cloud-Dienste auf verwalteten Windows-Geräten zu verwenden, und den Zugriff auf unerwünschte Cloud-Dienste blockieren. Diese Funktion ist nur in Kaspersky Security Center Web Console verfügbar.
- Die Abfrage des Domänencontrollers ermöglicht Ihnen jetzt das Abfragen von Samba-Domänencontrollern über einen Linux-basierten Verteilungspunkt. Zusätzliche Verbesserungen, welche die Abfrage großer Domänen unterstützen.
- Verbesserte Remote-Diagnose von verwalteten Linux-Geräten.
- Erweiterte Hardware-Inventur für macOS-Geräte. Der Administrationsagent auf einem macOS-Gerät sendet die MAC-Adresse und die Seriennummer des Geräts an den Administrationsserver.

- Sie können jetzt die Verbindungsherstellung mit SIEM-Systemen testen.
- Die maximale Länge des Kennworts für interne Benutzer wurde auf 256 Zeichen erhöht.
- Wenn Sie von Kaspersky Security Center Windows zu Kaspersky Security Center Linux migrieren, können Sie jetzt die verwalteten Geräte auf die Verwaltung durch Kaspersky Security Center Linux umstellen, indem Sie das Zertifikat und den privaten Schlüssel des Administrationsservers aus einer Backup-Kopie wiederherstellen
- Wenn Sie die Tool "Cleaner" oder "klmover" ausführen, um einen kennwortgeschützten Administrationsagenten zu entfernen, werden Sie aufgefordert, das Deinstallationskennwort einzugeben.
- Beim Upgrade von Kaspersky Security für Windows Server auf Kaspersky Endpoint Security für Windows ist kein Neustart des Zielgeräts mehr erforderlich.
- Ein Benutzer kann während oder nach der Installation des Administrationsagenten auf einem Linux-Client-Gerät zum Gerätebesitzer ernannt werden.
- Sie können jetzt einen Bericht über die Remote-Installation abrufen, wenn Sie Software über benutzerdefinierte Skripte auf den verwalteten Geräten installieren.
- Beim Ausführen mehrerer benutzerdefinierter Skripte auf einem verwalteten Gerät können Sie für jedes Skript eine Priorität festlegen, um die Ausführungsreihenfolge der Skripte zu definieren. Die Skripte werden der Reihe nach entsprechend ihrer Priorität ausgeführt, wobei mit das Skript mit der höchsten Priorität zuerst ausgeführt wird.
- Erweiterter Audit für Richtlinien. Sie können sich jetzt den Inhalt einer Richtlinienrevisionen anzeigen lassen und eine Richtlinienrevision in einer Datei speichern. Diese Funktionen sind derzeit nur für die Richtlinien des Administrationsservers und des Administrationsagenten verfügbar.
- Verbesserungen der Benutzerfreundlichkeit, einschließlich:
  - Das Hauptmenü lässt sich personalisieren, indem im Abschnitt **Angepinnt** ausgewählte Abschnitte der Kaspersky Security Center Web Console für einen schnelleren Zugriff angeheftet werden können.
  - Optimierter Umgang mit Tabellen. Die Standardansicht jeder Tabelle enthält jetzt die am häufigsten verwendeten Spalten. Außerdem können Sie jetzt alle Elemente der aktuellen Seite oder der gesamten Tabelle auswählen sowie die Elemente in der gesamten Tabelle sortieren.
  - Verbesserte Konfiguration der Berichtszustellung. Sie können jetzt bis zu 20 E-Mail-Adressen für die Empfänger des Berichts und den Zeitplan für die Zustellung des Berichts angeben.
- Sie können die lokalen Administratorrechte von Konten auf verwalteten Linux-Geräten widerrufen. Dies gibt Ihnen zusätzliche Kontrolle über die Benutzerkonten. Sie können beispielsweise die lokalen Administratorrechte entziehen, nachdem eine einmalige Zuweisung abgeschlossen wurde.
- Sie können auf verwalteten Linux-Geräten das Kennwort des lokalen Benutzerkontos ändern. Dies kann nützlich sein, wenn ein Benutzer das Kennwort seines lokalen Benutzerkontos vergisst oder wenn eine geplante Kennwortänderung durchgeführt wird.
- Im Unterabschnitt **Verwaltung von Benutzerzertifikaten** können Sie angeben, welche Stammzertifikate installiert werden sollen. Diese Zertifikate können beispielsweise verwendet werden, um die Authentizität von Websites oder Webservern zu überprüfen.
- Der Bericht über Netzwerkangriffe beinhaltet jetzt die MAC-Adresse und den Port des angreifenden Geräts.

- Eine neue Option, die interne Benutzer beim nächsten Anmeldeversuch an der Kaspersky Security Center Web Console dazu zu zwingt, ihr Kennwort zu ändern.
- Wenn Sie Ereignisse in CEF- oder LEEF-Formaten in ein SIEM-System exportieren, wird die kommerzielle Lizenz nicht mehr geprüft.
- Wenn Sie von einer Kaspersky-Anwendung auf eine andere migrieren möchten und Ihre aktuelle Anwendung durch ein Kennwort geschützt ist, können Sie jetzt das Kennwort für die Deinstallation in der Aufgabe zur Remote-Installationsaufgabe angeben.
- Exchange ActiveSync wird nicht mehr unterstützt.

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 enthält eine Reihe neuer Funktionen und Verbesserungen:

- Ein neuer Härtungsleitfaden wurde veröffentlicht. Wir empfehlen Ihnen dringend, den Leitfaden sorgfältig zu lesen und die Sicherheitsempfehlungen zu befolgen, um Kaspersky Security Center und Ihre Netzwerkinfrastruktur zu konfigurieren.

  Installieren Sie außerdem das neueste Update für Kaspersky Security Center. Dieses Update enthält Infrastruktur-Schutzfunktionen wie die zweistufige Überprüfung von Benutzerkonten und andere Verbesserungen.
- Der Zugriff auf Kaspersky-Server wird jetzt automatisch verifiziert. Wenn der Zugriff auf die Server über das systemspezifische DNS nicht möglich ist, verwendet das Programm ein öffentliches DNS.
- Die Benutzerrechte auf einem virtuellen Administrationsserver können unabhängig vom primären Administrationsserver jederzeit konfiguriert werden. Außerdem können Sie den Benutzern primärer Server die Rechte zum Verwalten eines virtuellen Servers zuweisen.
- Kaspersky Security Center unterstützt jetzt die folgenden DBMS:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (alle Editionen)
  - Postgres Pro 14.x (alle Editionen)
  - MariaDB 10.1, 10.4, 10.5
- Darüber hinaus stehen Ihnen in Kaspersky Security Center Web Console folgende Funktionen zur Verfügung: Export von Richtlinien und Aufgaben in eine Datei, und anschließender Import von Richtlinien und Aufgaben in Kaspersky Security Center Windows oder Kaspersky Security Center Linux.
- Die Option **Keinen Proxyserver verwenden** Option wurde aus den folgenden Aufgaben entfernt:
  - *Download von Updates in die Datenverwaltung des Administrationsservers*
  - *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*

- Um Client-Geräte in einer Cloud-Umgebung schützen, können Sie Kaspersky Endpoint Security für Windows anstelle von Kaspersky Security für Windows Server bereitstellen. Diese Funktion ist jetzt mit der Veröffentlichung von Kaspersky Endpoint Security 12.0 für Windows verfügbar.

- Das Arbeiten mit den Chiffrierschlüsseln wird jetzt durch die Zugriffsrechte für die den funktionalen Bereich **Allgemeine Funktionen**: **Verwaltung der Chiffrierschlüssel** eingeschränkt. Die Benutzer von Kaspersky Security Center können jetzt Chiffrierschlüssel exportieren, wenn sie über die Berechtigung **Lesen** verfügen, und importieren, wenn sie über die Berechtigung **Schreiben** verfügen.

Kaspersky Security Center 14

Kaspersky Security Center 14 enthält eine Reihe neuer Funktionen und Verbesserungen:

- Sie können Updates installieren und in einem isolierten Netzwerk Schwachstellen in Drittanbieter-Programme beheben (gilt nicht für Software von Microsoft). Solche Netzwerke umfassen Administrationsserver und verwaltete Geräte, die keinen Internetzugang haben. Um in einem solchen Netzwerk Schwachstellen zu beheben, müssen Sie die erforderlichen Updates über einen Administrationsserver mit Internetzugang herunterladen und die Patches dann an die isolierten Administrationsserver übertragen.

- Für macOS-Geräte wurden Verbindungsprofile für abwesende Benutzer hinzugefügt. Durch die Verwendung von Verbindungsprofilen können Sie die Regeln für Administrationsagenten auf macOS-Geräten so konfigurieren, dass diese je nach Gerätestandort eine Verbindung zum gleichen oder zu unterschiedlichen Administrationsservern herstellen.

- Der Administrationsagent kann jetzt auf Geräten, auf denen Microsoft Windows 10 IoT Enterprise läuft, installiert werden.

- Im **Bericht über Bedrohungen** können Sie jetzt die Bedrohungsliste so filtern, dass nur die durch Cloud Sandbox erkannten Bedrohungen angezeigt werden.

- Kaspersky Security Center unterstützt jetzt Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 als verwaltetes Programm.

Kaspersky Security Center Web Console enthält eine Reihe neuer Funktionen und Verbesserungen:

- Für Mitarbeiter, die das Netzwerk nicht verwalten, aber die Statistiken zum Netzwerkschutz in Kaspersky Security Center anzeigen möchten (z. B. ein Top-Manager) können Sie den Nur-Dashboard-Modus konfigurieren. Wenn dieser Modus bei einem Benutzer aktiviert ist, wird nur ein Dashboard mit einem vordefinierten Satz von Widgets angezeigt. So kann er oder sie die in den Widgets angegebenen Statistiken, wie den Schutzstatus aller verwalteten Geräte, die Anzahl der zuletzt erkannten Bedrohungen oder die Liste der häufigsten Bedrohungen im Netzwerk, überwachen.

- Kaspersky Security Center Web Console unterstützt jetzt Kaspersky Security für iOS als Sicherheitsanwendung.

- In den Aufgabeneigenschaften können Sie festlegen, ob Sie die Aufgabe auf Untergruppen und sekundäre Administrationsserver (auch virtuelle) anwenden möchten.

- Kaspersky Security Center unterstützt jetzt Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 als verwaltetes Programm.

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 enthält eine Reihe neuer Funktionen und Verbesserungen:

- Sie können jetzt den Administrationsserver, die Verwaltungskonsole, die Kaspersky Security Center 13.2 Web Console und den Administrationsagenten auf den folgenden zusätzlichen Betriebssystemen installieren (Mehr Informationen dazu in den Softwarevoraussetzungen):
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2 (Oktober 2021 Update)
  - Microsoft Server 2022
- Sie können MySQL 8.0 als Datenbank verwenden.
- Sie können Kaspersky Security Center auf einem Kaspersky Security Center Failover-Cluster bereitstellen, um eine hohe Verfügbarkeit von Kaspersky Security Center zu gewährleisten.
- Kaspersky Security Center kann jetzt neben IPv4-Adressen auch IPv6-Adressen verwalten. Der Administrationsserver kann Netzwerke abfragen, die Geräte mit IPv6-Adressen enthalten.

Kaspersky Security Center 13.2 Web Console enthält eine Reihe neuer Funktionen und Verbesserungen:

- Sie können jetzt mobile Android-Geräte mithilfe der Kaspersky Security Center 13.2 Web Console verwalten.
- Der Kaspersky Marketplace ist als neuer Menüeintrag verfügbar: Sie können jetzt direkt in der Kaspersky Security Center 13.2 Web Console nach neuen Kaspersky-Anwendungen suchen.
- Kaspersky Security Center unterstützt jetzt die folgenden Kaspersky-Anwendungen:
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 enthält eine Reihe neuer Funktionen und Verbesserungen:

- Die Integration in SIEM-Systeme wurde verbessert. Sie können jetzt Ereignisse über einen verschlüsselten Kanal (TLS) in SIEM-Systeme exportieren. Die Funktion ist für die Kaspersky Security Center Web Console und die MMC-basierte Verwaltungskonsole verfügbar.
- Sie können jetzt die Patches für den Administrationsserver als Programmpaket abrufen, welches Sie bei zukünftigen Upgrades auf höhere Versionen verwenden können.
- Der neue Abschnitt **Alarme** wurde für Kaspersky Endpoint Detection and Response Optimum zur Kaspersky Security Center 13.1 Web Console hinzugefügt. Außerdem wurden mehrere neue Widgets hinzugefügt, um mit den von Kaspersky Endpoint Detection and Response Optimum erkannten Bedrohungen umzugehen.

- In Kaspersky Security Center 13.1 Web Console können Sie Benachrichtigungen über ablaufende Lizenzen für Kaspersky-Anwendungen erhalten.

- Die Reaktionszeit von Kaspersky Security Center 13.1 Web Console wurde verbessert.

Kaspersky Security Center 13

Die folgenden Funktionen wurden Kaspersky Security Center 13 Web Console hinzugefügt:

- Die zweistufige Überprüfung wurde implementiert. Sie können die zweistufige Überprüfung aktivieren, um das Risiko eines nicht autorisierten Zugriffs auf die Kaspersky Security Center 13 Web Console zu verringern.

- Es wurde die Domänenauthentifizierung mithilfe der Protokolle NTLM und Kerberos (Single Sign-on) implementiert. Ein Windows-Benutzer, der die Funktion zum Single Sign-on verwendet, kann die sichere Authentifizierung in Kaspersky Security Center 13 Web Console aktivieren, ohne das Kennwort im Unternehmensnetzwerk erneut eingeben zu müssen.

- Sie können jetzt ein Plug-in für zur Integration von Kaspersky Managed Detection and Response konfigurieren. Sie können diese Integration verwenden, um Vorfälle anzuzeigen und Workstations zu verwalten.

- Sie können jetzt Einstellungen der Kaspersky Security Center 13 Web Console im Installationsassistenten des Administrationsservers festlegen.

- Es werden Benachrichtigungen über neu veröffentlichte Updates und Patches angezeigt. Sie können ein Update sofort oder jederzeit später installieren. Sie können jetzt Patches für den Administrationsserver mithilfe der Kaspersky Security Center 13 Web Console installieren.

- Wenn Sie mit Tabellen arbeiten, können Sie jetzt die Reihenfolge und Breite der Spalten angeben, Daten sortieren und die Seitengröße festlegen.

- Sie können jetzt einen beliebigen Bericht öffnen, indem Sie auf seinen Namen klicken.

- Kaspersky Security Center 13 Web Console ist jetzt in koreanischer Sprache verfügbar.

- Ein neuer Abschnitt namens Mitteilungen von Kaspersky, steht jetzt im Menü **Überwachung und Berichterstattung** zur Verfügung. Dieser Abschnitt informiert Sie über Wissenswertes zu Ihrer Version von Kaspersky Security Center und zu verwalteten Programmen, die auf den verwalteten Geräten installiert sind. Kaspersky Security Center aktualisiert die Informationen in diesem Abschnitt regelmäßig, indem veraltete Ankündigungen entfernt und neue Informationen hinzugefügt werden. Sie können die Mitteilungen von Kaspersky auch deaktivieren, wenn Sie möchten.

- Die zusätzliche Authentifizierung nach Änderungen von Einstellungen eines Benutzerkontos wurde implementiert. Sie können den Schutz vor unbefugten Änderungen für ein Benutzerkonto aktivieren. Wenn diese Option aktiviert ist, muss sich ein Benutzer mit Änderungsrechten autorisieren, um die Benutzerkonto-Einstellungen zu ändern.

Die folgenden Funktionen wurden Kaspersky Security Center 13 hinzugefügt:

- Die zweistufige Überprüfung wurde implementiert. Sie können die zweistufige Überprüfung aktivieren, um das Risiko eines nicht autorisierten Zugriffs auf die Verwaltungskonsole zu verringern. Wenn diese Option aktiviert ist, muss sich der Benutzer mit Änderungsrechten autorisieren, um die Benutzerkonto-Einstellungen zu ändern. Sie können jetzt die zweistufige Überprüfung für KES-Geräte aktivieren oder deaktivieren.

- Sie können über HTTP Nachrichten an den Administrationsserver senden. Für die Arbeit mit der OpenAPI des Administrationsservers sind jetzt ein Referenzhandbuch und eine Python-Bibliothek verfügbar.

- Sie können ein Reservezertifikat zur Verwendung in iOS MDM-Profilen ausstellen, um nach Ablauf des iOS MDM-Server-Zertifikats einen nahtlosen Wechsel verwalteter iOS-Geräte sicherzustellen.

- Der Ordner mit mandantenfähigen Anwendungen wird nicht mehr in der Verwaltungskonsole angezeigt.

Über Kaspersky Security Center

Dieser Abschnitt informiert über die Konzeption, die wichtigsten Funktionen, die Programmkomponenten und Vorgehensweisen zum Erwerb von Kaspersky Security Center.

Die Informationen in der Online-Hilfe unterscheiden sich eventuell von den Informationen in der Dokumentation, die zum Lieferumfang des Programms gehört. In diesem Fall gelten die Informationen der Online-Hilfe als aktuell. Sie können über die Links in der Programmoberfläche oder in der Dokumentation zur Online-Hilfe wechseln. Die Online-Hilfe kann ohne Ankündigung aktualisiert werden. Bei Notwendigkeit können Sie zwischen der Online-Hilfe und Offline-Hilfe wechseln.

Das Programm Kaspersky Security Center dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentral zu erledigen. Das Programm ermöglicht es dem Administrator, auf detaillierte Informationen über die Sicherheitsstufe des Unternehmensnetzwerks zuzugreifen und alle Schutzkomponenten anzupassen, die auf Kaspersky-Anwendungen basieren.

Kaspersky Security Center ist für Administratoren von Unternehmensnetzwerken und für Mitarbeiter gedacht, die für die Sicherheit von Geräten in Unternehmen verantwortlich sind.

Kaspersky Security Center bietet Ihnen folgende Möglichkeiten:

- Eine Hierarchie der Administrationsserver erstellen, um das eigene Unternehmensnetzwerk sowie Netzwerke entfernter Standorte bzw. Kundenunternehmen verwalten zu können.

  Mit *Kundenunternehmen* bezeichnet man Unternehmen, deren Antiviren-Schutz von Dienstanbietern gewährleistet wird.

- Eine Hierarchie der Administrationsgruppen erstellen, um eine Gruppe von bestimmten Client-Geräten als Ganzes zu verwalten.

- Antiviren-Schutz verwalten, der auf Kaspersky-Anwendungen basiert.

- Images von Betriebssystemen zentral erstellen und sie auf Client-Geräten eines Netzwerks verteilen sowie die Remote-Installation von Kaspersky-Programmen und Programmen anderer Softwarehersteller durchführen.

- Kaspersky-Programme und Programme anderer Hersteller, die auf Client-Geräten installiert wurden, von einem entfernten Standort verwalten: Updates installieren, Schwachstellen suchen und schließen.

- Zentralisierte Verteilung von Lizenzschlüsseln für Kaspersky-Anwendungen an die Client-Geräte, Überwachung der Verwendung von Lizenzschlüsseln, Verlängerung von Lizenzen.

- Statistiken und Berichte über die Ausführung von Anwendungen und Geräten abrufen.

- Benachrichtigungen über kritische Ereignisse bei der Ausführung von Kaspersky-Anwendungen empfangen.

- Verwaltung mobiler Geräte.

- Verwaltung der Verschlüsselung von Informationen, die auf Geräte-Festplatten und Wechseldatenträgern gespeichert werden, sowie den Zugriff der Benutzer auf verschlüsselte Daten.

- Inventarisierung der mit dem Unternehmensnetzwerk verbundenen Hardware durchführen.
- Dateien, die von den Sicherheitsanwendungen in die Quarantäne oder ins Backup verschoben wurden, sowie Dateien, deren Verarbeitung durch die Sicherheitsanwendungen aufgeschoben wurde, zentral verwalten.

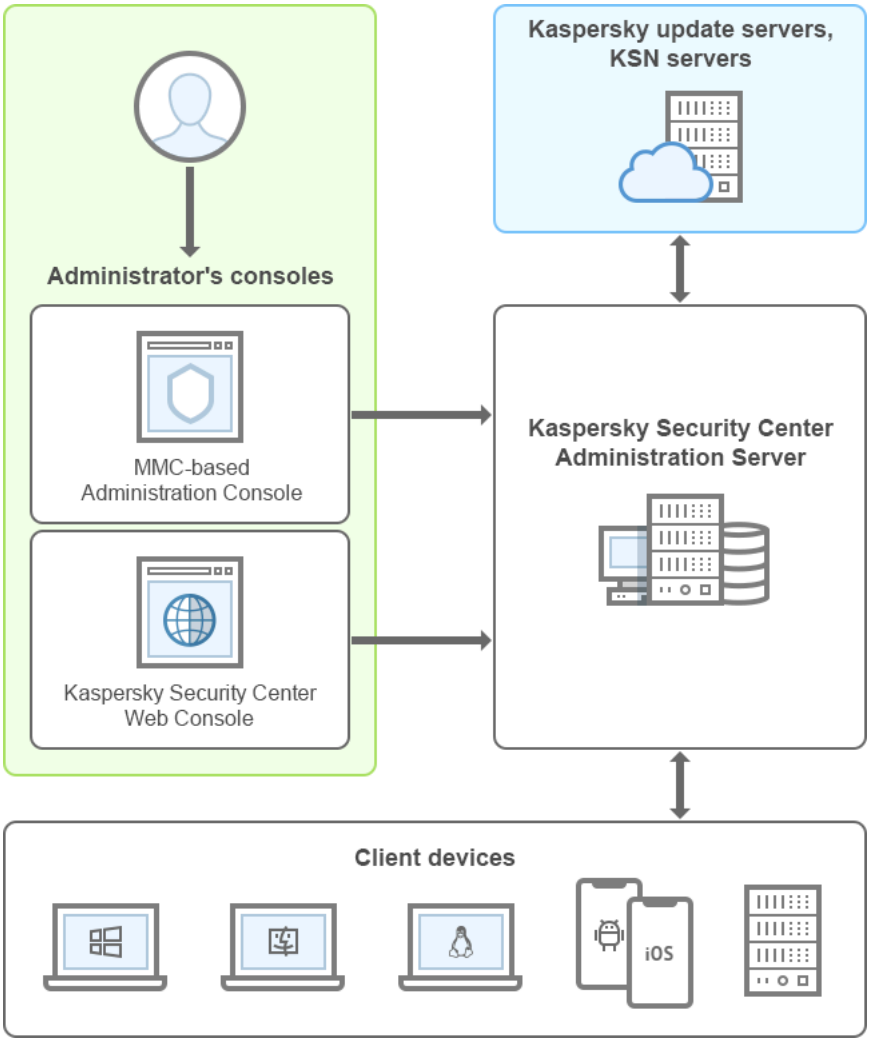
Sie können Kaspersky Security Center direkt bei Kaspersky (beispielsweise auf https://www.kaspersky.de) oder über unsere Partnerunternehmen erwerben.

Wenn Sie Kaspersky Security Center direkt über Kaspersky erwerben, können Sie das Programm von unserer Website herunterladen. Sie erhalten die zur Anwendungsaktivierung erforderlichen Informationen per E-Mail, nachdem der Eingang Ihres Rechnungsbetrags verarbeitet wurde.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Architektur

Dieser Abschnitt enthält eine Beschreibung der Komponenten von Kaspersky Security Center und deren Interaktion.



Architektur von Kaspersky Security Center

Kaspersky Security Center enthält die folgenden Basiskomponenten:

- *Verwaltungskonsole* (im Folgenden auch *Konsole*). Stellt die Benutzeroberfläche zu administrativen Diensten des Administrationsservers und des Administrationsagenten bereit. Die Verwaltungskonsole entspricht einer Erweiterungskomponente der Microsoft Management Console (MMC). Die Verwaltungskonsole ermöglicht das Herstellen einer Verbindung mit dem Remote-Administrationsserver über das Internet.

- *Kaspersky Security Center Web Console*. Bietet eine Weboberfläche zum Erstellen und Verwalten des Schutzsystems in dem von Kaspersky Security Center verwalteten Netzwerk des Kundenunternehmens.

- *Kaspersky Security Center Administrationsserver* (auch als *Server* bezeichnet). Führt die Funktionen zum zentralen Speichern von Daten über die im Firmennetzwerk installierten Anwendungen und deren Verwaltung aus.

- *Kaspersky-Update-Server*. HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule beziehen.

- *KSN-Server*. Server, die eine Datenbank von Kaspersky mit ständig aktualisierten Informationen über die Reputation von Dateien, Web-Ressourcen und Software umfassen. Kaspersky Security Network gewährleistet eine schnellere Reaktion der Kaspersky-Anwendungen auf Bedrohungen, erhöht die Leistungsfähigkeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

- *Client-Geräte*. Von Kaspersky Security Center geschützte Geräte des Kundenunternehmens. Auf jedem zu schützenden Gerät muss eine der Sicherheitsanwendungen von Kaspersky installiert sein.

Hard- und Softwarevoraussetzungen

- Anforderungen an den Administrationsserver
- Anforderungen an die Web Console
- Anforderungen an Server für mobile Geräte
- Anforderungen an die Verwaltungskonsole
- Anforderungen an den Administrationsagenten

Weitere Informationen über die Versionsanforderungen an Android und iOS zur Bereitstellung des Schutzes und die Verwaltung mobiler Geräte finden Sie in der Hilfe zu Kaspersky Security für mobile Endgeräte und Kaspersky Secure Mobility Management.

Anforderungen an den Administrationsserver

Mindestvoraussetzungen an die Hardware:

- Die CPU benötigt eine Taktfrequenz von 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1.4 GHz.
- RAM: 4 GB.
- Freier Speicherplatz auf dem Datenträger: 10 GB. Um das "Schwachstellen- und Patch-Management" verwenden zu können, müssen auf dem Laufwerk mindestens 100 GB freier Speicherplatz verfügbar sein.

Für die Bereitstellung in Cloud-Umgebungen entsprechen die Anforderungen an den Administrationsserver und den Datenbankserver den gleichen Anforderungen, wie an einen physischen Administrationsserver (in Abhängigkeit davon, wie viele Geräte Sie verwalten wollen).

Softwarevoraussetzungen:

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

Die folgenden Betriebssysteme werden unterstützt:

> Damit die Prozesse im Betriebssystem untereinander kommunizieren können, muss die Loopback-Schnittstelle verfügbar sein.

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-Bit
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installationsoption) (LTSB) 64-Bit
- Windows Server 2019 Standard/Datacenter/Core 64-Bit
- Windows Server 2022 Standard/Datacenter/Core 64-Bit
- Windows Server 2025 Standard/Datacenter/Core 64-Bit
- Windows Storage Server 2019 64-Bit

Die folgenden virtuellen Plattformen werden unterstützt:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 64-Bit

- Microsoft Hyper-V Server 2022 64-Bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

Die folgenden Datenbankserver werden unterstützt (Installation auf einem anderen Gerät möglich):

- Microsoft SQL Server 2016 (alle Editionen) 64-Bit
- Microsoft SQL Server 2017 (Alle Editionen) auf Windows/Linux 64-Bit
- Microsoft SQL Server 2019 (alle Editionen) auf Windows/Linux 64-Bit (Benötigt zusätzliche Maßnahmen)
- Microsoft SQL Server 2022 (Alle Editionen) auf Windows/Linux 64-Bit
- MySQL 5.7 Community 32-Bit/64-Bit
- MySQL Standard Edition 8.0 (Release 8.0.20 und höher) 32-Bit/64-Bit
- MySQL Enterprise Edition 8.0 (Release 8.0.20 und höher) 32-Bit/64-Bit
- MariaDB 10.5 (Build 10.5.27 und höher) 32-Bit/64-Bit
- MariaDB Galera Cluster 10.3 32-Bit/64-Bit mit InnoDB Storage Engine
- PostgreSQL 13.x 64-Bit
- PostgreSQL 14.x 64-Bit
- PostgreSQL 15.x 64-Bit
- Postgres Pro 13.x Windows/Linux 64-Bit
- Postgres Pro 14.x Windows/Linux 64-Bit

Informationen und Einschränkungen finden Sie im folgenden Thema: Auswahl des DBMS.

SIEM und andere Systeme zur Informations- und Ereignisverwaltung:

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

Anforderungen an die Web Console

Server der Kaspersky Security Center Web Console

Hardwaremindestvoraussetzungen:

- CPU: 4 Kerne, Taktfrequenz 2,5 GHz
- RAM: 8 GB
- Freier Speicherplatz auf dem Datenträger: 40 GB

Mindestanforderungen an die Zertifikate des Administrationsservers:

- SHA-2-Algorithmus für die Signatur des Zertifikats
- Minimale Schlüssellänge: 2048

Wenn Sie das Zertifikat erneut ausstellen müssen, finden Sie Informationen dazu in der Wissensdatenbank von Kaspersky Security Center.

Von Kaspersky Security Center Web Console Server unterstützte Betriebssysteme

Betriebssysteme. Microsoft Windows (nur 64-Bit-Versionen) Damit die Prozesse im Betriebssystem untereinander kommunizieren können, muss die Loopback-Schnittstelle verfügbar sein.	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installationsoption) (LTSB) Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019
Virtualisierungsplattformen	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

Client-Geräte

Für die Nutzung von Kaspersky Security Center Web Console auf einem Client-Gerät ist nur ein Browser erforderlich.

Die minimale Bildschirmauflösung beträgt 1366 x 768 Pixel.

Die Hard- und Softwarevoraussetzungen für das Gerät entsprechen den Anforderungen des Browsers, der für die Arbeit mit Kaspersky Security Center Web Console verwendet wird.

Browser:

- Google Chrome 128.0.6613.120 oder höher
- Microsoft Edge 128.0.2739.67 oder höher
- Safari 17.6 auf macOS
- Yandex Browser 24.7.3.1081 oder höher
- Mozilla Firefox Extended Support Release 115.14.0 oder höher

Anforderungen an Server für mobile Geräte

iOS Mobile Device Management Server (iOS MDM-Server)

Hardwarevoraussetzungen:

- Die CPU benötigt eine Taktfrequenz von 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1.4 GHz.
- RAM: 2 GB.
- Freier Speicherplatz auf dem Datenträger: 2 GB.

Betriebssystem Microsoft Windows (die Version des unterstützten Betriebssystems wird durch die Anforderungen des Administrationsservers bestimmt).

Anforderungen an die Verwaltungskonsole

Hardwarevoraussetzungen:

- Die CPU benötigt eine Taktfrequenz von 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1.4 GHz.
- RAM: 512 MB.
- Freier Speicherplatz auf dem Datenträger: 1 GB.

Softwarevoraussetzungen:

- Betriebssystem Microsoft Windows (die Version des unterstützten Betriebssystems wird durch die Anforderungen des Administrationsservers bestimmt):
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64-Bit
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) 64-Bit
  - Windows Server 2019 Standard/Datacenter 64-Bit

    - Windows Server 2022 Standard/Datacenter 64-Bit
    - Windows Server 2025 Standard/Datacenter/Core 64-Bit
    - Windows Storage Server 2019 64-Bit
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 ausgeführt auf:
    - Microsoft Windows Server 2012 R2
    - Microsoft Windows Server 2016
    - Microsoft Windows Server 2019
    - Microsoft Windows Storage Server 2019
- Microsoft Edge ausgeführt auf Microsoft Windows Server 2022 Standard

Anforderungen an den Administrationsagenten

Hardwaremindestvoraussetzungen:

- Die CPU benötigt eine Taktfrequenz von 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1.4 GHz.
- RAM: 512 MB.
- Freier Speicherplatz auf dem Datenträger: 1 GB.

Softwarevoraussetzung für Linux-basierte Geräte: Der Perl-Sprachinterpreter muss mindestens ab Version 5.10 installiert sein.

Betriebssysteme. Microsoft Windows	Windows Embedded POSReady 2009 mit dem aktuellsten Service Pack, 32-Bit Windows Embedded 7 Standard mit Service Pack 1 32-Bit/64-Bit Windows Embedded 8.1 Industry Pro 32-Bit/64-Bit Windows 10 Enterprise 2015 LTSB 32-Bit/64-Bit Windows 10 Enterprise 2016 LTSB 32-Bit/64-Bit Windows 10 IoT Enterprise 2015 LTSB 32-Bit/64-Bit Windows 10 IoT Enterprise 2016 LTSB 32-Bit/64-Bit Windows 10 Enterprise 2019 LTSC 32-Bit/64-Bit Windows 10 IoT Enterprise Version 1703 32-Bit/64-Bit Windows 10 IoT Enterprise Version 1709 32-Bit/64-Bit Windows 10 IoT Enterprise Version 1803 32-Bit/64-Bit Windows 10 IoT Enterprise Version 1809 32-Bit/64-Bit Windows 10 20H2 IoT Enterprise 32-Bit/64-Bit Windows 10 21H2 IoT Enterprise 32-Bit/64-Bit Windows 10 IoT Enterprise 32-Bit/64-Bit Windows 10 IoT Enterprise Version 1909 32-Bit/64-Bit Windows 10 IoT Enterprise LTSC 2021 32-Bit/64-Bit Windows 10 IoT Enterprise Version 1607 32-Bit/64-Bit Windows 10 TH1 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 TH2 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 RS1 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 RS3 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 RS5 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 19H1 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 20H1 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 21H1 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Windows 10 22H2 Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Windows 8 Pro/Enterprise 32-Bit/64-Bit Windows 8.1 Pro/Enterprise 32-Bit/64-Bit Windows 7 Home/Pro/Enterprise/Ultimate mit Service Pack 1 32-Bit/64-Bit Microsoft Windows XP Professional mit Service Pack 2 32-Bit/64-Bit (nur unterstützt durch den Administrationsagenten in Version 10.5.1781, die Sie über den Technischen Support anfordern können) Windows XP Professional mit Service Pack 3 und höher, 32-Bit (unterstützt vom Administrationsagenten in Version 14.0.0.20023) Windows XP Professional for Embedded Systems mit Service Pack 3 32-Bit (unterstützt vom Administrationsagenten in Version 14.0.0.20023) Windows MultiPoint Server 2011 Standard/Premium 64-Bit Windows Server 2003 SP1 32-Bit/64-Bit (nur unterstützt durch den Administrationsagenten in Version 10.5.1781) Windows Server 2003 SP2 Standard/Enterprise 32-Bit/64-Bit (nur unterstützt durch den Administrationsagenten in Version 10.5.1781) Windows Server 2003 R2 Standard/Enterprise with SP2 32-Bit/64-Bit (nur unterstützt vom Administrationsagenten Version 10.5.1781) Windows Server 2008 Standard/Enterprise/Datacenter/Foundation mit Service Pack 2 32-Bit/64-Bit Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation mit Service Pack 1 und höher, 64-Bit Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64-Bit Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-Bit

	Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installationsoption) (LTSB) 64-Bit Windows Server 2019 Standard/Datacenter/Core 64-Bit Windows Server 2019 RS5 Standard/Essentials 64-Bit Windows Server 2022 Standard/Datacenter/Core 64-Bit Windows Server 2022 21H2 Standard/Datacenter 64-Bit Windows Server 2025 Standard/Datacenter/Core 64-Bit Windows Storage Server 2019 64-Bit

Betriebssysteme. Linux	Debian GNU/Linux 10.x (Buster) 32-Bit/64-Bit Debian GNU/Linux 11.x (Bullseye) 32-Bit/64-Bit Debian GNU/Linux 12 (Bookworm) 32-Bit/64-Bit Ubuntu Server 18.04 LTS (Bionic Beaver) 64-Bit Ubuntu Server 20.04 LTS (Focal Fossa) 64-Bit Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-Bit Ubuntu Server 22.04 ARM 64-Bit Ubuntu Server 24.04 LTS (Noble Numbat) 64-Bit CentOS 6.7 und höher, 32-Bit CentOS 6.x (bis 6.6) 32-Bit/64-Bit CentOS 7.x 64-Bit CentOS Stream 8 64-Bit CentOS Stream 9 64-Bit CentOS Stream 9 ARM 64-Bit Red Hat Enterprise Linux Server 6.x 32-Bit/64-Bit Red Hat Enterprise Linux Server 7.x 64-Bit Red Hat Enterprise Linux Server 8.x 64-Bit Red Hat Enterprise Linux Server 9.x 64-Bit SUSE Linux Enterprise Server 12 (alle Service Packs) 64-Bit SUSE Linux Enterprise Server 15 (alle Service Packs) 64-Bit SUSE Linux Enterprise Server 15 (alle Service Packs) ARM 64-Bit openSUSE 15 64-Bit EulerOS 2.0 SP10 64-Bit EulerOS 2.0 SP10 ARM 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.5) 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.6) 64-Bit Astra Linux Special Edition RUSB.10015-16 (Release 1) (operatives Update 1.6) 64-Bit Astra Linux Special Edition RUSB.10015-17 (operatives Update 1.7.3) 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.7) 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8) 64-Bit Astra Linux Special Edition RUSB.10015-37 (operatives Update 7.7) 64-Bit Astra Linux Special Edition RUSB.10152-02 (operatives Update 4.7) ARM 64-Bit Astra Linux Common Edition (operatives Update 2.12) 64-Bit ALT Workstation 10.1 64-Bit ALT Server 10.1 64-Bit ALT Education 10.1 64-Bit ALT SP Server 10 32-Bit/64-Bit ALT SP Server 10 ARM 64-Bit ALT SP Workstation 10 32-Bit/64-Bit ALT SP Workstation 10 ARM 64-Bit ALT Server 10 64-Bit ALT Server 10 ARM 64-Bit ALT Workstation 10 32-Bit/64-Bit ALT 8 SP Workstation (8.4) ARM 64-Bit ALT 8 SP Server (8.4) ARM 64-Bit ALT 8 SP Server (LKNV.11100-01) 32-Bit/64-Bit ALT 8 SP Server (LKNV.11100-02) 32-Bit/64-Bit ALT 8 SP Server (LKNV.11100-03) 32-Bit/64-Bit ALT 8 SP Workstation (LKNV.11100-01) 32-Bit/64-Bit ALT 8 SP Workstation (LKNV.11100-02) 32-Bit/64-Bit ALT 8 SP Workstation (LKNV.11100-03) 32-Bit/64-Bit Mageia 4 32-Bit Oracle Linux 7 64-Bit Oracle Linux 8 64-Bit Oracle Linux 9 64-Bit Linux Mint 20.x 64-Bit

	Linux Mint 21.1 und höher, 64-Bit AlterOS 7.5 und höher, 64-Bit GosLinux IC6/7.17 64-Bit GosLinux IC6/7.2 64-Bit SberOS 3.3.1 64-Bit Plattform V SberLinux OS Server (SLO) 8.8 64-Bit Plattform V SberLinux OS Server (SLO) 8.9.2 64-Bit RED OS 7.3 ARM 64-Bit RED OS 7.3 Server 64-Bit RED OS 7.3 Certified Edition 64-Bit RED OS 8 Certified Edition 64-Bit ROSA Enterprise Linux Server 7.9 64-Bit ROSA Enterprise Linux Desktop 7.9 64-Bit ROSA COBALT 7.9 64-Bit ROSA CHROME 12 64-Bit AlmaLinux 8 und höher, 64-Bit AlmaLinux 9 und höher, 64-Bit Rocky Linux 8 und höher, 64-Bit Rocky Linux 9 und höher, 64-Bit Atlant, Alcyone-Build, Version 2022.02 64-Bit MSVSPHERE 9.2 SERVER 64-Bit MSVSPHERE 9.2 ARM 64-Bit SynthesisM Server 8.6 64-Bit SynthesisM Client 8.6 64-Bit OSnova 2.10 64-Bit Kylin 10 64-Bit EMIAS 1.0 64-Bit Amazon Linux 2 64-Bit MosOS 15.4 Arbat 64-Bit OS MES (Moscow Electronic School) 64-Bit
Betriebssysteme. macOS	Eine Liste der unterstützten Betriebssysteme finden Sie in der Hilfe zu Kaspersky Endpoint Security for Mac.

Für den Administrationsagenten werden außerdem sowohl die Architektur "Apple Silicon (M1)" als auch Intel unterstützt.

Die folgenden virtuellen Plattformen werden unterstützt:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM (Kernel-basierte virtuelle Maschine)

Bei Windows-Versionen, die älter als Microsoft Windows Server 2008 R2 (Server-Versionen) und Microsoft Windows 7 (Desktop-Versionen) sind, unterstützt der Administrationsagent die folgenden Funktionen nicht:

- Übertragen von Updates and die Geräte (von Verteilungspunkten verwendet)
- KSN-Proxy (von Verteilungspunkten verwendet)
- Aufgabe zur Untersuchung auf Schwachstellen

Auf Geräten mit Microsoft Windows 10 Version RS4 oder RS5 kann es vorkommen, dass Kaspersky Security Center nicht in der Lage ist, Schwachstellen zu finden, wenn diese sich in Ordnern mit aktivierter Unterscheidung zwischen Groß- und Kleinschreibung befinden.

Stellen Sie vor der Installation des Administrationsagenten auf Geräten mit Windows 7, Windows Server 2008 oder Windows Server 2008 R2 sicher, dass Sie das Sicherheitsupdate KB3063858 für Windows-Betriebssysteme installiert haben (Sicherheitsupdate für Windows 7 (KB3063858), Sicherheitsupdate für Windows 7 für Systeme auf x64-Basis (KB3063858), Sicherheitsupdate für Windows Server 2008 (KB3063858), Sicherheitsupdate für Windows Server 2008 x64 Edition (KB3063858), Sicherheitsupdate für Windows Server 2008 R2 x64 Edition (KB3063858).

Unter Windows XP führt der Administrationsagent einige Vorgänge möglicherweise nicht korrekt aus.

Sie können den Administrationsagenten für Windows XP nur unter Microsoft Windows XP installieren oder aktualisieren. Die unterstützten Editionen von Microsoft Windows XP und die entsprechenden Versionen des Administrationsagenten sind in der Liste mit unterstützten Betriebssystemen aufgeführt. Sie können die erforderliche Version des Administrationsagenten für Microsoft Windows XP von dieser Seite herunterladen.

Es wird empfohlen, den Administrationsagenten in der gleichen Version wie zu installieren, wie Kaspersky Security Center.

Kaspersky Security Center bietet vollständige Unterstützung für die Administrationsagenten derselben oder neuerer Versionen.

Der Administrationsagent für macOS wird zusammen mit der Kaspersky-Sicherheitsanwendung für dieses Betriebssystem bereitgestellt.

Kompatible Anwendungen und Lösungen von Kaspersky

Kaspersky Security Center unterstützt die zentralisierte Bereitstellung und Verwaltung aller derzeit unterstützten Kaspersky-Anwendungen und -Lösungen. Die folgende Tabelle enthält die Kaspersky-Anwendungen und -Lösungen, die von der MMC-basierten Verwaltungskonsole und der Kaspersky Security Center Web Console unterstützt werden. Genaue Informationen über die Versionen der Anwendungen und Lösungen finden Sie auf der Webseite für den Produktlebenszyklus.

Liste mit Anwendungen und Lösungen von Kaspersky, die von Kaspersky Security Center unterstützt werden

Name der Anwendung oder der Lösung von Kaspersky	Von der MMC-basierten Verwaltungskonsole unterstützt	Von der Kaspersky Security Center Web Console unterstützt
Für Workstations		
Kaspersky Endpoint Security für Windows	✓	✓
Kaspersky Endpoint Security für Linux	✓	✓
Kaspersky Endpoint Security für Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security für Windows	✓	✓
Kaspersky Embedded Systems Security für Linux	—	✓
Für industrielle Lösungen		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (zentralisierte Bereitstellung wird nicht unterstützt)	✓	✓
Für mobile Geräte		
Kaspersky Endpoint Security für Android	✓	✓
Kaspersky Security für iOS	—	✓
Für Dateiserver		
Kaspersky Security für Windows Server	✓	✓
Kaspersky Endpoint Security für Windows	✓	✓
Kaspersky Endpoint Security für Linux	✓	✓
Für virtuelle Umgebungen		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	—
Zum Erkennen zielgerichteter Angriffe		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
Für Geräte mit KasperskyOS		
Kaspersky IoT Secure Gateway	—	✓
Kaspersky Thin Client	—	✓
Reputations-Datenbanken		
Kaspersky Private Security Network	—	✓

Lizenzen und Funktionen von Kaspersky Security Center 15.1

Kaspersky Security Center erfordert für einige seiner Funktionen eine Lizenz.

Die folgende Tabelle zeigt, welche Funktionen von Kaspersky Security Center durch welche Lizenz abgedeckt werden.

Um die Funktionen von Kaspersky Security Center zu aktivieren, müssen Sie den Administrationsserver aktivieren, indem Sie dem Administrationsserver einen Lizenzschlüssel hinzufügen.

Ein Lizenzschlüssel muss für jeden Administrationsserver manuell hinzugefügt werden.

Lizenzen und Funktionen von Kaspersky Security Center

Funktionen von Kaspersky Security Center	Kaspersky Schwachstellen- und Patch-Management	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
Schwachstellenbewertung	✓	✓	✓	✓	✓	✓	✓
Patch-Management	✓	–	✓	✓	–	✓	✓
Rollenbasierte Zugriffskontrolle	✓	✓	✓	✓	✓	✓	✓
Installation von Betriebssystemen und Programmen	✓	–	✓	✓	–	✓	✓
Verwaltung mobiler Geräte (d.h. Verwaltung der iOS- und Android-Geräte der Benutzer)	✓	✓	✓	✓	–	–	✓
Umgebung zur Cloud-Konfiguration für die Arbeit in Cloud-Umgebungen wie AWS, Microsoft Azure oder Google Cloud	–	–	–	–	✓	✓	–
Exportieren von Ereignissen in SIEM-Systeme: Syslog	✓	✓	✓	✓	✓	✓	✓
Exportieren von Ereignissen in SIEM-Systeme: QRadar von IBM und ArcSight von Micro Focus	✓	✓	✓	✓	✓	✓	✓

Über die Kompatibilität der Kaspersky Security Center-Komponenten

Die folgende Tabelle enthält Informationen zur Kompatibilität der Komponenten von Kaspersky Security Center.

Kompatibilität der Komponenten von Kaspersky Security Center

Komponente	Kompatibel mit
Kaspersky Security Center 15.1 Administrationsserver	• Kaspersky Security Center 15.1 Verwaltungskonsole • Kaspersky Security Center 15.1 Web Console. • Kaspersky Security Center Administrationsagent in den Versionen 16.2, 16.1, 16, 15.4, 15.1, 15, 14.2, 14.
Kaspersky Security Center 15.1 Web Console	Kaspersky Security Center Administrationsserver in den Versionen 15.1 und 14.2.

Komponente	Kompatibel mit
Kaspersky Security Center 15.1 Primärer Administrationsserver	Sekundäre Administrationsserver: • Kaspersky Security Center 14 Windows • Kaspersky Security Center 14.2 Windows • Kaspersky Security Center 15.1 Windows • Kaspersky Security Center 14.2 Linux • Kaspersky Security Center 15 Linux • Kaspersky Security Center 15.1 Linux
Kaspersky Security Center 15.1 Sekundärer Administrationsserver	Primäre Administrationsserver: • Kaspersky Security Center 14 Windows • Kaspersky Security Center 14.2 Windows • Kaspersky Security Center 15.1 Windows • Kaspersky Security Center 14.2 Linux • Kaspersky Security Center 15 Linux • Kaspersky Security Center 15.1 Linux

Es wird empfohlen, sowohl den Kaspersky Security Center Administrationsserver als auch die Kaspersky Security Center Web Console in der jeweils aktuellsten Version zu verwenden. Andernfalls wird die Funktionalität von Kaspersky Security Center möglicherweise eingeschränkt. Sie können den Kaspersky Security Center Administrationsserver und die Kaspersky Security Center Web Console unabhängig voneinander installieren und aktualisieren. In diesem Fall müssen Sie sicherstellen, dass die Version der installierten Kaspersky Security Center Web Console mit der Version des Administrationsservers, mit dem Sie eine Verbindung herstellen, kompatibel ist:

Wenn Sie über die neueste Version von Kaspersky Security Center Web Console und eine frühere Version von Kaspersky Security Center verwenden und während der Domänenauthentifizierung ein Fehler auftritt, enthält der Fehlertext eine Standardmeldung.

Vergleich von Kaspersky Security Center: Windows-basiert vs. Linux-basiert

Kaspersky bietet Kaspersky Security Center als lokale Lösung für zwei Plattformen – Windows und Linux. Bei der Windows-basierten Lösung installieren Sie den Administrationsserver auf einem Windows-Gerät und bei der Linux-basierten Lösung ist die Administrationsserver-Version für die Installation auf einem Linux-Gerät vorgesehen. Diese Online-Hilfe enthält Informationen zu Kaspersky Security Center Windows. Ausführliche Informationen zur Linux-basierten Lösung finden Sie in der Online-Hilfe von Kaspersky Security Center Linux.

Die folgende Tabelle bietet einen Vergleich der Hauptfunktionen von Kaspersky Security Center als Windows-basierte Lösung und als Linux-basierte Lösung.

Funktionsvergleich von Kaspersky Security Center als Windows-basierte Lösung und Linux-basierte Lösung

Funktion oder Eigenschaft	Kaspersky Security Center	
	Windows-basierte Lösung	Linux-basierte Lösung
Administrationsserver		
Standort des Datenbankmanagementsystems (DBMS)	On-premises	On-premises (Microsoft SQL wird nicht unterstützt)
Betriebssystem, auf dem der Administrationsserver installiert werden soll	Windows	Linux
Hierarchie des Administrationsservers	✓	✓

Funktion oder Eigenschaft	Kaspersky Security Center	
	Windows-basierte Lösung	Linux-basierte Lösung
Unterstützung für virtuelle Administrationsserver	✓	✓
Verwenden von SNMP, um Administrationsserver-Statistiken an Drittanbieter-Programme zu senden	✓	Wird im Jahr 2026 implementiert
Webserver zum Veröffentlichen von Installationspaketen und anderen Dateien	✓	✓
Installation des Administrationsservers in einem Single-Site Failover-Cluster auf Basis von Windows Server	✓	—
Kaspersky Security Center Failover-Cluster bereitstellen	✓ Nur ein Single-Site-Cluster	✓ Ab Kaspersky Security Center 16.2 Linux werden geografisch verteilte Failover-Cluster unterstützt.
Verwaltungskonsole		
Typ der Verwaltungskonsole	MMC-basiert und webbasiert	Webbasiert
Betriebssystem, auf dem die webbasierte Verwaltungskonsole installiert werden soll	Windows oder Linux	Linux
Anmelden an der Konsole mit Domänenauthentifizierung	✓	✓ Einmaliges Anmelden (Single Sign-on) wird für die Versionen 15.1 bis einschließlich 15.4 nicht unterstützt.
Verwaltung von Client-Geräten und Administrationsgruppen		
Maximale Anzahl verwalteter Geräte (pro Administrationsserver)	100.000	50.000 (mit PostgreSQL und Postgres Pro)
Netzwerkabfrage	✓	✓ Beginnend mit Version 16 werden FreeIPA- und ALD Pro-Domänencontroller unterstützt
Schutz von verwalteten Windows-, macOS- und Linux-verwalteten Geräten	✓	✓
Schutz von mobilen Geräten	✓ Grundlegende Verwaltung mobiler Geräte	✓ MDM und Verwendung der Funktionen von Kaspersky Secure Mobility Management (unter Lizenz)
Verwaltung des Schutzes von virtuellen Maschinen	✓	✓
Schutz der Public-Cloud-Infrastruktur	✓	—
Remote-Desktopverbindung mit einem Client-Gerät	✓	✓ Ab Version 15.3
Verschlüsselung und Datenschutz	✓	✓ Auf Windows-basierten verwalteten Geräten mit installiertem Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security for Mac
Unterstützung von Clustern und Server-Arrays in Administrationsgruppen	✓	✓
Hierarchie der Administrationsgruppen	✓	✓
Hinzufügen eines Verbindungs-Gateways als Verteilungspunkt innerhalb der DMZ	✓ (MMC-basierte Verwaltungskonsole)	Wird im Jahr 2026 implementiert
Benutzerverwaltung		
Erstellen und Verwalten von Benutzerkonten	✓	✓
Verwaltung von Kaspersky-Anwendungen		
Anwendungsrichtlinien	✓	✓

Funktion oder Eigenschaft	Kaspersky Security Center	
	Windows-basierte Lösung	Linux-basierte Lösung
Aufgaben für Kaspersky-Anwendungen	✓	✓
Kaspersky Security Network	✓	✓
KSN-Proxy	✓	✓
Kaspersky Private Security Network	✓	✓
Zentralisierte Bereitstellung von Lizenzschlüsseln für Kaspersky-Anwendungen	✓	✓
Ferndiagnose der Client-Geräte	✓	✓
Automatisches Aktualisieren der Kaspersky-Anwendungen	✓	✓
Unterstützung der Adaptiven Kontrolle von Anomalien	✓	✓
Gerätezentrierte Sicherheitsverwaltung	✓	✓
Benutzerzentrierte Sicherheitsverwaltung	✓	✓
Systemverwaltung		
Bereitstellen von Betriebssystemen auf Client-Geräten	✓	—
Verwalten der Lizenzen von Drittanbietern	✓	—
Administrationsserver als WSUS-Server verwenden	✓	✓ (Nur im passivem Modus für die Suche nach Windows-Updates)
Verwalten von Programmen von Drittanbietern auf Client-Geräten		
Installieren von Updates für Drittanbieter-Programme und Beheben von Schwachstellen in Drittanbieter-Programmen	✓	✓
Überwachung, Berichterstattung und Audit		
Umgang mit Objekt-Revisionen	✓	✓
Vergleichen von Richtlinienrevisionen	✓	Wird im Jahr 2026 implementiert
Anzeigen und Bearbeiten der Alarme, die von Kaspersky Endpoint Detection and Response Optimum erkannt wurden	✓	✓
Benachrichtigungen über Ereignisse, die auf verwalteten Geräten auftreten	✓	✓
Überwachung des Richtlinienstatus und Aufgabenstatus	✓	✓
Integrationen		
Integration mit Kaspersky Managed Detection and Response	✓	✓
Integration von SIEM-Systemen	✓	✓
Exportieren von Ereignissen mittels CEF- und LEEF-Formaten	✓	✓
Aggregation von Alarmen und Ausführen von Reaktionsmaßnahmen über Active Directory, KASAP und Kaspersky TIP Sandbox	—	✓ (Ab Version 15.4) Sie müssen den Administrationsserver mit einer Lizenz für Kaspersky Next XDR Optimum aktivieren und anschließend den Lizenzschlüssel von Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereitstellen.

Über die Kaspersky Security Center Cloud Console

Die Verwendung von Kaspersky Security Center als lokal installierte Anwendung (on-premises) bedeutet, dass Sie Kaspersky Security Center zusammen mit dem Administrationsserver auf einem lokalen Gerät installieren, und die Netzwerksicherheit entweder über die auf der Microsoft Management Console basierenden Verwaltungskonsole (nur für Kaspersky Security Center Windows verfügbar) oder über die Kaspersky Security Center Web Console verwalten.

Alternativ dazu können Sie Kaspersky Security Center auch als Cloud-Dienst verwenden. In diesem Fall wird für Sie Kaspersky Security Center von Kaspersky-Experten in einer Cloud-Umgebung installiert und verwaltet, und Kaspersky gewährt Ihnen den Zugriff auf den Administrationsserver in Form eines Dienstes. Sie verwalten die Netzwerksicherheit durch eine cloudbasierte Verwaltungskonsole namens Kaspersky Security Center Cloud Console. Die Benutzeroberfläche dieser Konsole ist ähnlich der von Kaspersky Security Center Web Console.

Die Benutzeroberfläche und Dokumentation von Kaspersky Security Center Cloud Console sind in folgenden Sprachen verfügbar:

- Englisch
- Französisch
- Deutsch
- Italienisch
- Japanisch
- Portugiesisch (Brasilien)
- Russisch
- Vereinfachtes Chinesisch
- Spanisch
- Spanisch (LATAM)
- Traditionelles Chinesisch

Weitere Informationen zu Kaspersky Security Center Cloud Console und seinen Funktionen finden Sie in der Dokumentation von Kaspersky Security Center Cloud Console und in der Dokumentation von Kaspersky Endpoint Security for Business.

Kaspersky Security Center 15.1

In diesem Abschnitt finden Sie Informationen über die Arbeit mit dem Programm Kaspersky Security Center 15.1.

Die Informationen in der Online-Hilfe unterscheiden sich eventuell von den Informationen in der Dokumentation, die zum Lieferumfang des Programms gehört. In diesem Fall gelten die Informationen der Online-Hilfe als aktuell. Sie können über die Links in der Programmoberfläche oder in der Dokumentation zur Online-Hilfe wechseln. Die Online-Hilfe kann ohne Ankündigung aktualisiert werden. Bei Notwendigkeit können Sie zwischen der Online-Hilfe und Offline-Hilfe wechseln.

Grundbegriffe

Dieser Abschnitt enthält ausführliche Definitionen der Grundbegriffe zu Kaspersky Security Center.

Administrationsserver

Die Komponenten von Kaspersky Security Center ermöglichen eine Remote-Programmverwaltung der auf Client-Geräten installierten Kaspersky-Anwendungen.

Geräte, auf welchen die Komponente "Administrationsserver" installiert ist, werden als *Administrationsserver* bezeichnet (im Weiteren auch *Server* genannt). Administrationsserver müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Der Administrationsserver wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Unter dem Namen "Kaspersky Security Center Administrationsserver"
- Mit automatischem Start bei Start des Betriebssystems
- Unter dem Benutzerkonto **LocalSystem** oder unter dem Benutzerkonto, das bei Installation des Administrationsservers ausgewählt wurde

Der Administrationsserver führt folgende Funktionen aus:

- Speicherung der Struktur der Administrationsgruppen
- Speicherung von Informationen über die Konfiguration der Client-Geräte
- Organisation der Datenverwaltung für Anwendungspakete
- Remote-Installation von Anwendungen auf Client-Geräten und Löschen von Anwendungen
- Datenbanken-Update und Update der Module von Kaspersky-Anwendungen
- Verwaltung von Richtlinien und Aufgaben auf Client-Geräten

- Speicherung von Informationen über die auf den Client-Geräten aufgetretenen Ereignisse
- Erstellen von Berichten über die Ausführung von Kaspersky-Anwendungen
- Verteilung von Lizenzschlüsseln auf Client-Geräte, sowie Speicherung von Informationen über die Lizenzschlüssel
- Senden von Benachrichtigungen über den Status der Aufgabenausführung (z. B. über einen Virenfund auf einem Client-Gerät)

Namensgebung für Administrationsserver in der Programmoberfläche

In den Oberflächen der MMC-basierten Verwaltungskonsole und in der Kaspersky Security Center Web Console können Administrationsserver die folgenden Namen haben:

- Name des Geräts mit dem Administrationsserver, z. B. "*Gerätename*" oder "Administrationsserver: *Gerätename*".
- IP-Adresse des Geräts mit dem Administrationsserver, z. B. "*IP-Adresse*" oder "Administrationsserver: *IP-Adresse*".
- Sekundäre Administrationsserver und virtuelle Administrationsserver haben benutzerdefinierte Namen, die Sie beim Verbinden eines virtuellen oder sekundären Administrationsservers mit dem primären Administrationsserver angeben.
- Wenn Sie Kaspersky Security Center Web Console auf einem Linux-Gerät installiert haben und verwenden, zeigt das Programm die Namen von Administrationsservern, die Sie als "vertrauenswürdig" eingestuft haben, in einer Antwort-Datei an.

Das Herstellen einer Verbindung zum Administrationsserver via Verwaltungskonsole oder Kaspersky Security Center Web Console ist jeweils möglich.

Hierarchie des Administrationsservers

Administrationsserver können eine Hierarchie bilden. Jeder Administrationsserver kann über mehrere sekundäre Administrationsserver (im Folgenden auch *sekundäre Server*) auf verschiedenen Hierarchieebenen verfügen. Die Verschachtelungstiefe der sekundären Server ist nicht beschränkt. Zu den Administrationsgruppen des primären Administrationsservers gehören die Client-Geräte aller sekundärer Administrationsserver. So können unabhängige Bereiche des Computernetzwerks durch verschiedene Administrationsserver verwaltet werden, die wiederum durch einen primären Server administriert werden.

Ein *virtueller Administrationsserver* stellt einen besonderen Fall eines sekundären Administrationsservers dar.

Die Hierarchie der Administrationsserver lässt sich zu folgenden Zwecken verwenden:

- Beschränkung der Belastung des Administrationsservers (im Vergleich zu einem einzigen im Netzwerk installierten Server).
- Verringerung des Datenverkehrs im Netzwerk und Vereinfachung der Arbeit mit Remote-Niederlassungen. Sie müssen keine Verbindungen zwischen dem primären Administrationsserver und allen Geräten im Netzwerk herstellen, die sich zum Beispiel in anderen Regionen befinden können. Es genügt, wenn in jedem Segment des Netzwerks ein sekundärer Administrationsserver installiert ist, die Geräte auf Administrationsgruppen der sekundären Server verteilt werden und für die sekundären Server schnelle Verbindungen zum primären Server bestehen.

- Verteilung der Verantwortung zwischen den Administratoren für den Antiviren-Schutz. Dabei bleiben alle Möglichkeiten der zentralen Verwaltung und der Überwachung des Status des Antiviren-Schutzes im Unternehmensnetzwerk erhalten.

- Verwendung von Kaspersky Security Center über Dienstanbieter. Ein Dienstanbieter muss lediglich Kaspersky Security Center und die Kaspersky Security Center Web Console installieren. Um eine große Anzahl an Client-Geräten verschiedener Unternehmen zu verwalten, kann der Dienstanbieter sekundäre Administrationsserver (einschließlich sekundärer Server) zur Hierarchie der Administrationsserver hinzufügen.

Jedes Gerät, das zur Hierarchie der Administrationsgruppen gehört, kann nur mit einem Administrationsserver verbunden sein. Sie müssen die Verbindung der Geräte mit den Administrationsservern selbständig prüfen. Dazu können Sie die Suche-Funktion der Geräte nach Netzwerkattributen in den Administrationsgruppen verschiedener Server verwenden.

Virtueller Administrationsserver

Ein virtueller Administrationsserver (im Folgenden auch *Virtueller Server* genannt) ist eine Komponente des Programms Kaspersky Security Center, die dazu konzipiert ist, den Antiviren-Schutz im Netzwerk eines Kundenunternehmens zu verwalten.

Ein virtueller Administrationsserver stellt einen besonderen Fall eines sekundären Administrationsservers dar und weist im Vergleich zu einem physikalischen Administrationsserver folgende Einschränkungen auf:

- Ein virtueller Administrationsserver kann nur auf einem primären Administrationsserver erstellt werden.

- Ein virtueller Administrationsserver verwendet während seines Betriebs die Datenbank des primären Administrationsservers. Aufgaben zum Anlegen eines Daten-Backups und zur Wiederherstellung von Dateien, sowie Aufgaben zur Suche nach Updates und Downloadaufgaben werden von einem virtuellen Administrationsserver nicht unterstützt.

- Für virtuelle Server können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).

Außerdem weisen virtuelle Administrationsserver folgende Einschränkungen auf:

- Im Eigenschaftenfenster des virtuellen Administrationsservers ist die Anzahl der Abschnitte beschränkt.

- Um eine Remote-Installation von Kaspersky-Anwendungen auf Client-Geräten vorzunehmen, die vom virtuellen Administrationsserver verwaltet werden, muss auf einem der Computer der Administrationsagent installiert sein, über den eine Verbindung zum virtuellen Administrationsserver aufgebaut werden kann. Beim ersten Verbindungsaufbau zum virtuellen Administrationsserver wird diesem Computer automatisch die Rolle des Verteilungspunkts zugewiesen, sodass er als Verbindungs-Gateway für den Anschluss von Client-Geräten an den virtuellen Administrationsserver dient.

- Der virtuelle Server kann das Netzwerk nur über die Verteilungspunkte durchsuchen.

- Um einen virtuellen Server neu zu starten, der in seiner Funktionsfähigkeit beeinträchtigt wurde, startet Kaspersky Security Center den primären Administrationsserver und alle virtuellen Administrationsserver neu.
- Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Der Administrator eines virtuellen Administrationsservers verfügt über alle Rechte für diesen virtuellen Server.

Server für mobile Geräte

Beim *Server für mobile Geräte* handelt es sich um eine Komponente von Kaspersky Security Center, die den Zugriff auf mobile Geräte bietet und deren Verwaltung über die Verwaltungskonsole ermöglicht. Der Server für mobile Geräte empfängt Informationen über mobile Geräte und speichert ihre Profile.

Kaspersky Security Center beinhaltet den iOS MDM-Server als Server für mobile Geräte. Mit diesem Server für mobile Geräte können Sie mobile Geräte verwalten, die den Dienst Apple® Push Notification (APNs) unterstützen.

Die Server für mobile Geräte von Kaspersky Security Center ermöglichen Ihnen, folgende Objekte zu verwalten:

- Ein einzelnes mobiles Gerät.
- Mehrere mobile Geräte.
- Mehrere mobile Geräte, die mit einem Server-Cluster verbunden sind (können gleichzeitig verwaltet werden). Bei der Verbindung mit einem Server-Cluster wird der in diesem Cluster installierte Server für mobile Geräte als ein einzelner Server in der Verwaltungskonsole angezeigt.

Webserver

Beim Kaspersky Security Center *Webserver* (im Folgenden auch *Webserver* genannt) handelt es sich um eine Kaspersky Security Center Komponente, die zusammen mit dem Administrationsserver installiert wird. Der Webserver dient dazu, autonome Installationspakete, iOS MDM-Profile sowie Dateien aus einem freigegebenen Ordner im Netzwerk zu übertragen.

Beim Erstellen wird ein autonomes Installationspaket automatisch auf dem Webserver veröffentlicht. Der Link für den Download des autonomen Paketes wird in der Liste der erstellten autonomen Installationspakete angezeigt. Bei Bedarf können Sie die Veröffentlichung des autonomen Paketes abbrechen oder es erneut auf dem Webserver veröffentlichen.

Beim Erstellen eines iOS MDM-Profils für das mobile Gerät eines Benutzers wird das Profil automatisch auf dem Webserver veröffentlicht. Das veröffentlichte Profil wird nach der erfolgreichen Installation auf dem mobilen Gerät des Benutzers automatisch vom Webserver gelöscht.

Der freigegebene Ordner wird zum Speichern von Informationen verwendet, die für alle Benutzer verfügbar sind, deren Geräte über den Administrationsserver verwaltet werden. Hat ein Benutzer keinen direkten Zugriff auf den freigegebenen Ordner, können die Informationen aus diesem Ordner mithilfe des Webservers an ihn übermittelt werden.

Um Informationen aus dem freigegebenen Ordner mithilfe des Webservers an Benutzer übermitteln zu können, soll der Administrator im Ordner einen Unterordner mit dem Namen public erstellen und die Informationen in diesen Unterordner kopieren.

Der Link für die Übermittlung der Informationen an den Benutzer soll folgendes Aussehen aufweisen:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

wobei:

- `<Web Server name>` für den Namen des Kaspersky Security Center Webservers.
- `<HTTPS port>` für den vom Administrator angegebenen HTTPS-Port des Webservers steht. Den HTTPS-Port können Sie im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers festlegen. Standardmäßig wird Portnummer 8061 verwendet.
- Beim `<object>` handelt es sich um einen Unterordner bzw. eine Datei, die für den Benutzer freigegeben werden sollen.

Der Administrator kann den erstellten Link auf jede Weise an den Benutzer übermitteln, wie etwa per E-Mail.

Mit diesem Link kann der Benutzer die für ihn vorgesehenen Informationen auf das lokale Gerät herunterladen.

Administrationsagent

Interaktion zwischen dem Administrationsserver und Geräten wird mithilfe der Komponente *Administrationsagent* von Kaspersky Security Center durchgeführt. Der Administrationsagent muss auf allen Geräten installiert werden, auf denen Kaspersky-Anwendungen mit Kaspersky Security Center verwaltet werden.

Der Administrationsagent wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Unter dem Namen "Kaspersky Security Center Administrationsagent"
- Mit automatischem Start bei Start des Betriebssystems
- Unter Verwendung des Kontos "LocalSystem"

Ein Gerät, auf dem der Administrationsagent installiert ist, wird als *verwaltetes Gerät* oder *Gerät* bezeichnet.

Sie können den Administrationsagenten auf einem Gerät mit Windows, Linux oder Mac installieren. Sie erhalten die Komponente aus einer der folgenden Quellen:

- Installationspaket im Speicher des Administrationsservers (dazu müssen Sie den Administrationsserver installiert haben)
- Installationspaket auf den Kaspersky-Webservern

Sie müssen den Administrationsagenten installieren nicht auf dem Gerät installieren, auf dem Sie den Administrationsserver installieren, da die Serverversion des Administrationsagenten automatisch gemeinsam mit dem Administrationsserver installiert wird.

Der Name des Prozesses, den der Administrationsagent startet, lautet *klnagent.exe*.

Der Administrationsagent synchronisiert das verwaltete Gerät mit dem Administrationsserver. Es wird empfohlen, das Synchronisierungsintervall (auch als *Herzschlag* bezeichnet) auf 15 Minuten pro 10.000 verwaltete Geräte einzurichten.

Administrationsgruppen

Bei einer *Administrationsgruppe* (im Folgenden *Gruppe* genannt) handelt es sich um einen logischen Satz von verwalteten Geräte, die nach einem beliebigen Merkmal zusammengefasst sind und als geschlossene Einheit innerhalb von Kaspersky Security Center verwaltet werden können.

Alle verwalteten Geräte innerhalb einer Administrationsgruppe sind für folgende Aktionen konfiguriert:

- Verwenden derselben Anwendungseinstellungen (die Sie in Gruppenrichtlinien festlegen können).
- Verwenden eines allgemeinen Betriebsmodus für alle Anwendungen, indem Gruppenaufgaben mit festgelegten Einstellungen erstellt werden. Beispiele für Gruppenaufgaben umfassen unter anderem das Erstellen und Installieren eines Standard-Installationspakets, Aktualisieren von Datenbanken und Modulen von Anwendungen, Untersuchung des Geräts auf Befehl und Aktivieren des Echtzeitschutzes.

Ein verwaltetes Gerät kann nur zu einer Administrationsgruppe gehören.

Sie können Hierarchien erstellen, die einen beliebige Tiefe für die Verschachtelung der Administrationsserver und der Gruppen aufweisen. Auf einer Hierarchieebene können sich sekundäre und virtuelle Administrationsserver sowie Gruppen und verwaltete Geräte befinden. Sie können Geräte von einer Gruppe zu einer anderen verschieben, ohne sie physikalisch zu bewegen. Wenn sich beispielsweise die Position eines Mitarbeiters im Unternehmen von Buchhalter auf Entwickler ändert, können Sie das Gerät dieses Mitarbeiters von der Administrationsgruppe "Buchhalter" in die Administrationsgruppe "Entwickler" verschieben. Anschließend erhält das Gerät automatisch die Programmeinstellungen, die für Entwickler erforderlich sind.

Verwaltetes Gerät

Ein *verwaltetes Gerät* ist entweder ein Gerät, das mit Windows, Linux oder macOS läuft und auf dem der Administrationsagent installiert ist, oder ein mobiles Gerät, auf dem eine Kaspersky-Sicherheitsanwendung installiert ist. Sie können solche Geräte verwalten, indem Sie Aufgaben und Richtlinien für auf diesen Geräten installierte Anwendungen erstellen. Sie können auch Berichte von verwalteten Geräten beziehen.

Sie können ein nicht-mobil verwaltetes Gerät als Verteilungspunkt und als Verbindungs-Gateway nutzen.

Ein Gerät kann nur von einem Administrationsserver verwaltet werden. Ein Administrationsserver kann bis zu 100.000 Geräte verwalten, einschließlich mobiler Geräte.

Nicht zugeordnetes Gerät

Ein *nicht zugeordnetes Gerät* ist ein Gerät im Netzwerk, dass in keine Administrationsgruppe aufgenommen wurde. Sie können mit den nicht zugeordneten Geräten Aktionen ausführen und sie z. B. in Administrationsgruppen verschieben oder Anwendungen darauf installieren.

Wenn ein neues Gerät in Ihrem Netzwerk gefunden wird, gelangt dieses Gerät in die Administrationsgruppe **Nicht zugeordnete Geräte**. Sie können Regeln für Geräte anpassen, die automatisch in andere Administrationsgruppen verschoben werden sollen, nachdem die Geräte ermittelt wurden.

Administrator-Arbeitsplatz

Der *Administrator-Arbeitsplatz* ist ein Gerät, auf dem die Verwaltungskonsole installiert ist, oder das Sie zum Öffnen der Kaspersky Security Center Web Console verwenden. Von diesen Geräten aus können die Administratoren eine zentralisierte Remote-Programmverwaltung für die auf den Client-Geräten installierten Kaspersky-Anwendungen durchführen.

Nachdem die Verwaltungskonsole auf Ihrem Gerät installiert wurde, wird ihr Symbol angezeigt, was Ihnen ermöglicht, die Verwaltungskonsole zu starten. Nach der Installation der Verwaltungskonsole erscheint auf Ihrem Gerät im Menü **Start** → **Programme** → **Kaspersky Security Center** das Symbol für den Start.

Die Anzahl an Administrator-Arbeitsplätzen ist nicht beschränkt. Von jedem Administrator-Arbeitsplatz aus können Administrationsgruppen mehrerer Administrationsserver zugleich verwaltet werden. Der Administrator-Arbeitsplatz kann mit dem Administrationsserver (physischen oder virtuellen) einer beliebigen Hierarchieebene verbunden werden.

Der Administrator-Arbeitsplatz kann in eine Administrationsgruppe als Client-Gerät aufgenommen werden.

Im Rahmen von Administrationsgruppen eines beliebigen Servers kann dasselbe Gerät sowohl Client des Administrationsservers als auch Administrationsserver und Administrator-Arbeitsplatz sein.

Verwaltungs-Plug-in

Die Kaspersky-Anwendungen werden über die Verwaltungskonsole mithilfe einer speziellen Komponente mit dem Namen *Verwaltungs-Plug-in* verwaltet. Alle Kaspersky-Anwendungen, die über Kaspersky Security Center verwaltet werden können, umfassen ein Verwaltungs-Plug-in.

Mithilfe des Plug-ins für die Programmverwaltung können Sie über die Verwaltungskonsole folgende Aktionen ausführen:

- Richtlinien erstellen sowie Programmeinstellungen und Aufgabeneinstellungen des Programms bearbeiten.
- Informationen über Programmaufgaben und Ereignisse, die während der Programmausführung auftreten, sowie Statistiken zur Programmausführung von Client-Geräten abrufen.

Sie können die Verwaltungs-Plug-ins von der Webseite des Technischen Supports von Kaspersky herunterladen.

Web-Plug-ins zur Verwaltung

Für die Remote-Verwaltung der Software von Kaspersky mithilfe von Kaspersky Security Center Web Console wird eine spezielle Komponente – das *Web-Plug-in zur Verwaltung* – verwendet. Im Weiteren wird das Web-Plug-in zur Verwaltung als *Verwaltungs-Plug-in* bezeichnet. Das Verwaltungs-Plug-in ist eine Schnittstelle zwischen Kaspersky Security Center Web Console und einer spezifischen Kaspersky-Anwendung. Mit einem Verwaltungs-Plug-in können Sie Aufgaben und Richtlinien für die Anwendung konfigurieren.

Sie können die Web-Plug-ins zur Verwaltung von der Kaspersky-Website herunterladen.

Das Verwaltungs-Plug-in stellt Folgendes bereit:

- Schnittstelle zum Erstellen und Ändern von Aufgaben und Einstellungen für Anwendungen
- Schnittstelle zum Erstellen und Ändern von Richtlinien und Richtlinienprofilen für die ferngesteuerte und zentralisierte Konfiguration von Kaspersky-Anwendungen und Geräten
- Übertragung von Ereignissen, die von der Anwendung erzeugt wurden
- Kaspersky Security Center Web Console funktioniert für die Anzeige von Betriebsdaten und Ereignissen der Anwendung sowie von Statistiken, die von Client-Geräten weitergeleitet wurden

Richtlinien

Eine *Richtlinie* besteht aus einer Reihe von Einstellungen für Kaspersky-Anwendungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Anwendungen auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center bietet eine einzelne Richtlinie für jede Kaspersky-Anwendung in einer Administrationsgruppe. Eine Richtlinie besitzt einen der folgenden Statuswerte (siehe Abbildung unten):

Status der Richtlinie

Status	Beschreibung
Aktiv	Die aktuelle Richtlinie, die auf das Gerät angewendet wird. In jeder Administrationsgruppe kann nur eine Richtlinie für eine Kaspersky-Anwendung aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für eine Kaspersky-Anwendung an.
Inaktiv	Eine Richtlinie, die derzeit nicht auf ein Gerät angewendet wird.
Für mobile Benutzer	Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

Richtlinien funktionieren gemäß den folgenden Regeln:

- Für eine einzelne Anwendung können mehrere Richtlinien mit unterschiedlichen Werten konfiguriert werden.
- Für das aktuelle Programm kann nur eine Richtlinie aktiv sein.
- Bei Auftreten eines bestimmten Ereignisses können Sie eine deaktivierte Richtlinie aktivieren. Dadurch können beispielsweise strengere Einstellungen des Antiviren-Schutzes bei Virenangriffen festgelegt werden.
- Eine Richtlinie kann untergeordnete Richtlinien haben.

Im Allgemeinen können Sie Richtlinien als Vorbereitung für Notfallsituationen wie Virenangriffe verwenden. Beispiel: Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. In diesem Fall wird die aktuell aktive Richtlinie automatisch inaktiv.

Um zu verhindern, dass mehrere Richtlinien verwaltet werden, können Sie beispielsweise Richtlinienprofile verwenden, wenn bei verschiedenen Gelegenheiten nur bestimmte Einstellungen geändert werden müssen.

Ein *Richtlinienprofil* stellt eine benannte Teilmenge von Einstellungswerten einer Richtlinie dar, welche die Einstellungswerte in einer Richtlinie ersetzen. Ein Richtlinienprofil wirkt sich auf die effektive Formation der Einstellungen auf einem verwalteten Gerät aus. *Effektive Einstellungen* stellen eine Zusammenstellung an Einstellungen für Richtlinien, Richtlinienprofile und lokalen Anwendungseinstellungen dar, die derzeit für das Gerät angewendet werden.

Richtlinienprofile funktionieren entsprechend den folgenden Regeln:

- Ein Richtlinienprofil wird wirksam, wenn eine bestimmte Aktivierungsbedingung auftritt.
- Richtlinienprofile enthalten Werte für Einstellungen, die von den Richtlinieneinstellungen abweichen.
- Durch das Aktivieren eines Richtlinienprofils werden die effektiven Einstellungen des verwalteten Gerätes geändert.
- Eine Richtlinie kann nicht mehr als 100 Richtlinienprofile enthalten.

Richtlinienprofile

Es kann manchmal erforderlich werden, in verschiedenen Administrationsgruppen mehrere Instanzen einer einzigen Richtlinie zu erstellen. Bei Bedarf können Sie die Einstellungen dieser Richtlinien auch zentral bearbeiten. Diese Instanzen können sich nur durch ein oder zwei Einstellungen unterscheiden. Beispielsweise arbeiten alle Buchhalter in einem Unternehmen unter derselben Richtlinie, leitende Buchhalter dürfen jedoch USB-Flash-Drives verwenden, was reguläre Buchhalter nicht dürfen. In diesem Fall ist die Übernahme von Richtlinien für Geräte ausschließlich gemäß der Hierarchie von Administrationsgruppen möglicherweise unpraktisch.

Damit Sie nicht mehrere Instanzen einer einzelnen Richtlinie erstellen müssen, ermöglicht es Ihnen Kaspersky Security Center, *Richtlinienprofile* zu erstellen. Richtlinienprofile sind erforderlich, wenn Sie möchten, dass Geräte innerhalb einer Administrationsgruppe unter verschiedenen Richtlinieneinstellungen ausgeführt werden.

Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von der "zugrundeliegenden" Richtlinie unterscheiden, die auf dem verwalteten Gerät aktiv ist. Die Aktivierung eines Profils ändert die Einstellungen der "zugrundeliegenden" Richtlinie, die ursprünglich auf dem Gerät aktiv waren. Die geänderten Einstellungen nehmen die im Profil festgelegten Werte an.

Aufgaben

Kaspersky Security Center verwaltet die auf Geräten installierten Sicherheitsanwendungen von Kaspersky durch das Erstellen und Starten von *Aufgaben*. Die Aufgaben ermöglichen Installation, Start und Beenden von Anwendungen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Anwendungsmodule sowie Ausführung anderer Aktionen mit den Anwendungen.

Aufgaben für eine bestimmte Anwendung können nur erstellt werden, sofern das Verwaltungs-Plug-in für diese Anwendung installiert ist.

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Die folgenden Aufgaben werden auf dem Administrationsserver ausgeführt:

- Berichte automatisch versenden
- Updates in die Datenverwaltung des Administrationsservers herunterladen
- Backup der Daten des Administrationsservers anlegen

- Datenbank bedienen
- Windows-Updates synchronisieren
- Installationspaket anhand des Betriebssystem-Abbilds eines Mustergeräts erstellen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

- *Lokale Aufgaben* sind Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

  Lokale Aufgaben können nicht nur vom Administrator mithilfe der Verwaltungskonsole geändert werden, sondern auch vom Benutzer des Remote-Geräts (beispielsweise in der Benutzeroberfläche der Sicherheitsanwendung). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

- *Gruppenaufgaben* sind Aufgaben, die auf allen Geräten einer bestimmten Gruppe ausgeführt werden.

  Soweit in den Aufgabeneigenschaften nicht anders festgelegt, betrifft eine Gruppenaufgabe auch alle Untergruppen der ausgewählten Gruppe. Eine Gruppenaufgabe betrifft (optional) auch Geräte, die mit den sekundären und virtuellen Administrationsservern in der Gruppe und den Untergruppen verbunden sind.

- *Globale Aufgaben* sind Aufgaben, die auf einem Satz von Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Gruppe gehören.

Sie können für jede Anwendung eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt von Aufgaben verfolgen, und Aufgaben kopieren, exportieren, importieren und löschen.

Eine Aufgabe wird auf einem Gerät nur dann gestartet, wenn das Programm gestartet wurde, für das diese Aufgaben erstellt worden waren.

Ergebnisse von Aufgaben werden Microsoft Windows Ereignisprotokoll und im Ereignisprotokoll von Kaspersky Security Center sowohl zentral auf dem Administrationsserver als auch lokal auf jedem Gerät gespeichert.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Aufgabenumfang

Der *Gültigkeitsbereich einer Aufgabe* ist der Satz von Geräten, auf denen die Aufgabe ausgeführt wird. Es gibt folgende Arten von Gültigkeitsbereichen:

- Für eine *lokale Aufgabe* ist der Gültigkeitsbereich das Gerät selbst.
- Für eine *Aufgabe des Administrationsservers* ist der Gültigkeitsbereich der Administrationsserver.
- Für eine *Gruppenaufgabe* ist der Gültigkeitsbereich die Liste der Geräte, die in der Gruppe enthalten sind.

Beim Erstellen einer *globalen Aufgabe* können Sie die folgenden Methoden verwenden, um ihren Gültigkeitsbereich festzulegen:

- Bestimmte Geräte manuell festlegen.

  Als Adresse des Geräts können Sie eine IP-Adresse (oder einen IP-Bereich), den NetBIOS- oder den DNS-Namen verwenden.

- Geräteliste aus einer txt-Datei mit den hinzuzufügenden Geräteadressen importieren (jede Adresse muss in einer eigenen Zeile stehen).

  Wenn Sie eine Geräteliste aus einer Datei importieren oder eine Liste manuell erstellen, und wenn die Geräte namentlich identifiziert werden, darf die Liste nur Geräte enthalten, deren Daten bereits in die Datenbank des Administrationsservers eingegeben wurden. Darüber hinaus müssen die Informationen entweder während einer bestehenden Verbindung der Geräte oder während einer Gerätesuche eingegeben worden sein.

- Geräteauswahl angeben.

  Im Laufe der Zeit ändert sich der Gültigkeitsbereich der Aufgabe, je nachdem, wie sich die Anzahl der Geräte ändert, die zur Auswahl gehören. Die Geräteauswahl kann aufgrund der Geräte-Attribute, einschließlich aufgrund der auf dem Gerät installierten Software, und aufgrund der dem Gerät zugewiesenen Tags strukturiert sein. Die Geräteauswahl ist die flexibelste Art zum Festlegen des Gültigkeitsbereichs einer Aufgabe.

  Aufgaben für die Geräteauswahlen werden immer nach Zeitplan durch den Administrationsserver ausgeführt. Solche Aufgaben werden auf Geräten, die keine Verbindung mit dem Administrationsserver haben, nicht ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden direkt auf Geräten ausgeführt und sind daher nicht von der Geräteverbindung zum Administrationsserver abhängig.

  Aufgaben für Geräteauswahlen werden nicht nach der lokalen Uhrzeit des Geräts, sondern nach der lokalen Uhrzeit des Administrationsservers ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden nach der lokalen Uhrzeit eines Geräts ausgeführt.

Interaktion von Richtlinien und lokalen Programmeinstellungen

Mit Richtlinien können identische Werte für Einstellungen einer Anwendung für alle Geräte gesetzt werden, die zu einer Gruppe gehören.

Die Einstellungswerte, die eine Richtlinie vorgibt, lassen sich für einzelne Geräte mit lokalen Anwendungseinstellungen ändern. Dabei können Werte nur für die Einstellungen festgelegt werden, deren Änderung nicht durch die Richtlinie unterbunden ist, d.h. wenn die Einstellung nicht durch ein verriegeltes Schloss blockiert wird.

Der Wert, den die Anwendung auf dem Client-Gerät verwendet wird durch die Position des Schlosses (🔒) für diese Richtlinieneinstellung definiert:

- Wenn die Änderung der Einstellung unterbunden ist, wird auf allen Client-Geräten der gleiche Wert verwendet, der von der Richtlinie vorgegeben ist.

- Wenn die Änderung nicht unterbunden ist, verwendet die Anwendung den lokalen Einstellungswert auf jedem Client-Gerät und nicht den Wert, der in der Richtlinie angegeben ist. Der Einstellungswert kann dabei über die lokalen Anwendungseinstellungen geändert werden.

Dies bedeutet, das bei Ausführung einer Aufgabe auf dem Client-Gerät die Anwendung Einstellungen anwendet, die auf zwei verschiedene Arten vorgegeben wurden:

- Durch die Aufgabeneinstellungen und die lokalen Anwendungseinstellungen, wenn die Änderung der Einstellung in der Richtlinie nicht unterbunden wurde.
- Durch die Gruppenrichtlinie, wenn die Änderung der Einstellung gesperrt wurde.

Die lokalen Anwendungseinstellungen werden nach der ersten Anwendung der Richtlinie mit den Richtlinieneinstellungen überschrieben.

Verteilungspunkt

Der *Verteilungspunkt* (früher: Update-Agent) ist ein Gerät mit installiertem Administrationsagenten, der für die Verteilung von Updates, die Remote-Installation von Programmen und den Empfang von Informationen über Geräte im Netzwerk verwendet wird. Verteilungspunkte beschleunigen die Update-Verteilung und ermöglichen, die Belastung des Administrationsservers zu verringern.

Die Funktionen und Anwendungsfälle eines Administrationsagenten, der auf einem Gerät installiert ist, das als Verteilungspunkt fungiert variieren je nach Betriebssystem.

Der Verteilungspunkt kann folgende Funktionen ausführen:

- Dateien, die vom Administrationsserver heruntergeladen wurden, auf die Client-Geräte der Gruppe verteilen (einschließlich Verteilung durch Multicasting über das UDP-Protokoll).

  Die Liste der Dateien, die von Verteilungspunkten übertragen werden können, umfasst:

  - Updates für die Datenbanken und Programm-Module von Kaspersky
  - Updates für Drittanbieter-Programme
  - Installationspakete
  - Windows-Updates, wenn Sie Administrationsserver als WSUS-Server verwenden

  Updates können sowohl vom Administrationsserver als auch von den Kaspersky-Update-Servern empfangen werden. Im letzteren Fall muss für den Verteilungspunkt eine Update-Aufgabe erstellt werden. Geräte mit Verteilungspunkten unter macOS können keine Updates von Kaspersky Update-Servern herunterladen.

  Wenn ein oder mehrere Geräte, die unter macOS laufen, in den Bereich der Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* fallen, schließt die Aufgabe mit dem Status *Fehlgeschlagen* ab, selbst wenn sie auf allen Windows-Geräten erfolgreich abgeschlossen wurde.

  Wenn alle Verteilungspunkte, die einem Gerät zugewiesen wurden, fehlerhaft sind, erhält das Gerät keine Updates (Antiviren-Datenbanken und Patches) und keine Installationspakete.

- Verteilen von Richtlinien und Gruppenaufgaben mittels Multicast über das UDP-Protokoll.

- Rolle des Gateways für die Verbindung mit dem Administrationsserver für Geräte in einer Administrationsgruppe übernehmen.

  Wenn keine Möglichkeit besteht, eine direkte Verbindung zwischen den verwalteten Geräten und dem Administrationsserver herzustellen, können Sie den Verteilungspunkt zum Gateway für Verbindungen dieser Gruppe mit dem Administrationsserver bestimmen. In diesem Fall werden die verwalteten Geräte mit dem Verbindungs-Gateway verbunden, das seinerseits mit dem Administrationsserver verbunden wird.

  Das Vorhandensein eines Verteilungspunkts, der die Rolle des Verbindungs-Gateways übernimmt, schließt eine direkte Verbindung der verwalteten Geräte mit dem Administrationsserver nicht aus. Wenn das Verbindungs-Gateway nicht verfügbar ist, aber eine direkte Verbindung mit dem Administrationsserver möglich ist, werden die verwalteten Geräte direkt mit dem Server verbunden.

- Abfragen des Netzwerks, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden. Der Verteilungspunkt kann dieselben Methoden zur Gerätesuche ausführen wie der Administrationsserver.

- Führen Sie die Remote-Installation von Drittanbieter-Programmen und Kaspersky-Anwendungen mithilfe der Tools des Betriebssystems des Verteilungspunkts durch. Beachten Sie, dass der Verteilungspunkt die Installation auf Client-Geräten ohne Administrationsagenten durchführen kann.

  Diese Funktion ermöglicht es, Installationspakete des Administrationsagenten auf Client-Geräte zu übertragen, die sich in Netzwerken befinden, auf die der Administrationsserver nicht direkt zugreifen kann.

- Als Proxyserver fungieren, der am Kaspersky Security Network (KSN) teilnimmt.

  Sie können den KSN-Proxyserver auf dem Verteilungspunkt aktivieren, damit das Gerät als KSN-Proxyserver agiert. In diesem Fall wird der KSN-Proxy-Service (ksnproxy) auf dem Gerät gestartet.

Die Übertragung von Dateien vom Administrationsserver an den Verteilungspunkt wird über das HTTP-Protokoll oder das HTTPS-Protokoll (wenn die Verwendung von SSL-Verbindungen konfiguriert ist) realisiert. Die Verwendung des HTTP- oder HTTPS-Protokolls gewährleistet im Vergleich zum SOAP-Protokoll aufgrund des reduzierten Datenverkehrs eine höhere Leistung.

Geräte mit installiertem Administrationsagenten können entweder manuell (vom Administrator) oder automatisch (vom Administrationsserver) zum Verteilungspunkt bestimmt werden. Eine vollständige Liste der Verteilungspunkte für die angegebenen Administrationsgruppen wird im Bericht über die Liste der Verteilungspunkte angezeigt.

Der Gültigkeitsbereich des Verteilungspunkts umfasst die Administrationsgruppe, für die der Verteilungspunkt vom Administrator bestimmt wurde, sowie ihre Untergruppen auf jeder Ebene der Verschachtelung. Wurden in der Hierarchie der Administrationsgruppen mehrere Verteilungspunkte bestimmt, wird der Administrationsagent des verwalteten Geräts mit dem Verteilungspunkt verbunden, der sich in der Hierarchie am nächsten befindet.

Als Gültigkeitsbereich des Verteilungspunkts kann auch ein Netzwerkstandort dienen. Der Netzwerkstandort wird zum Erstellen einer manuellen Auswahl von Geräten verwendet, auf die der Verteilungspunkt die Updates verteilt. Der Netzwerkspeicherort kann nur für Geräte mit Windows-Betriebssystem bestimmt werden.

Wenn die Verteilungspunkte automatisch vom Administrationsserver bestimmt werden, erfolgt dies anhand der Broadcast-Domänen und nicht anhand der Administrationsgruppen. Dies geschieht nachdem die Broadcast-Domäne bestimmt wurde. Der Administrationsagent führt einen Nachrichtenaustausch mit den anderen Administrationsagenten seines Subnetzes aus und sendet dem Administrationsserver Informationen über sich sowie Kurzinformationen über die anderen Administrationsagenten. Auf der Grundlage dieser Informationen kann der Administrationsserver eine Gruppierung der Administrationsagenten anhand der Broadcast-Domänen durchführen. Die Broadcast-Domänen werden dem Administrationsserver bekannt, nachdem mehr als 70 % der Administrationsagenten in den Administrationsgruppen durchsucht wurden. Der Administrationsserver durchsucht die Broadcast-Domänen alle zwei Stunden. Nachdem die Verteilungspunkte anhand der Broadcast-Domänen bestimmt wurden, können sie nicht mehr neu anhand von Administrationsgruppen bestimmt werden.

Wenn der Administrator die Verteilungspunkte manuell zuweist, können diese Verwaltungsgruppen oder Netzwerkstandorten zugewiesen werden.

Administrationsagenten mit aktivem Verbindungsprofil nehmen nicht an der Bestimmung der Broadcast-Domäne teil.

Kaspersky Security Center weist jedem Administrationsagenten die eindeutige Adresse für IP-Versand an mehrere Adressen zu, die sich nicht mit anderen Adressen überschneidet. Dadurch kann eine Überschreitung der Netzwerkbelastung vermieden werden, die aufgrund der Überkreuzung von IP-Adressen entstehen könnte.

Wenn in einem Netzwerksegment oder einer Administrationsgruppe zwei oder mehr Verteilungspunkte bestimmt werden, wird einer davon aktiv, und die anderen bleiben in Reserve. Der aktive Verteilungspunkt lädt Updates und Installationspakete unmittelbar vom Administrationsserver herunter, während die Reserve-Verteilungspunkte nur den aktiven Verteilungspunkt nach Updates abfragen. In diesem Fall werden Dateien nur einmal vom Administrationsserver heruntergeladen und im Weiteren auf die Verteilungspunkte verteilt. Sollte der aktive Verteilungspunkt aus irgendwelchen Gründen offline sein, wird einer der Reserve-Verteilungspunkte zum aktiven bestimmt. Der Administrationsserver bestimmt die Reserve-Verteilungspunkte automatisch.

Der Status eines Verteilungspunkts (*Aktiv*/*Reserve*) wird mittels eines Kontrollkästchens im Bericht des Tools klnagchk angezeigt.

Für die Ausführung des Verteilungspunkts sind mindestens 4 GB freier Speicherplatz auf dem Datenträger erforderlich. Wenn der freie Speicherplatz auf dem Datenträger des Verteilungspunkts weniger als 2 GB beträgt, erstellt Kaspersky Security Center einen Sicherheitsvorfall der Ereigniskategorie *Warnung*. Der Sicherheitsvorfall wird in den Eigenschaften des Geräts im Abschnitt **Sicherheitsprobleme** veröffentlicht.

Für die Ausführung von Aufgaben zur Remote-Installation ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher freier Speicherplatz auf dem Datenträger erforderlich. Der freie Speicherplatz sollte größer sein als der Gesamtumfang aller zu installierenden Installationspakete.

Für die Ausführung der Aufgaben zur Installation von Updates (Patches) und zum Schließen von Schwachstellen ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher freier Speicherplatz auf dem Datenträger erforderlich. Der freie Speicherplatz sollte mindestens doppelt so groß sein wie der Gesamtumfang aller zu installierenden Patches.

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Verbindungs-Gateway

Ein *Verbindungs-Gateway* ist ein Administrationsagent, der in einem speziellen Modus ausgeführt wird. Ein Verbindungs-Gateway akzeptiert Verbindungen von anderen Administrationsagenten und tunnelt diese zum Administrationsserver mittels einer eigenen Verbindung zum Server. Anstatt wie gewöhnliche Administrationsagenten selbst eine Verbindung zum Administrationsserver herzustellen, wartet ein Verbindungs-Gateway auf eine Verbindung vom Administrationsserver.

Ein Verbindungs-Gateway kann bis zu 10.000 Verbindungen von Geräten empfangen.

Sie haben zwei Möglichkeiten, Verbindungs-Gateways zu verwenden:

- Wir empfehlen, dass Sie ein Verbindungs-Gateway in einer entmilitarisierten Zone (DMZ) installieren. Für andere Administrationsagenten, die auf mobilen Geräten installiert sind, müssen Sie explizit eine Verbindung zum Administrationsserver über das Verbindungs-Gateway konfigurieren.

  Ein Verbindungs-Gateway ändert oder verarbeitet in keiner Weise Daten, die von Administrationsagenten an den Administrationsserver übertragen werden. Es schreibt darüber hinaus keinerlei Daten in einen Puffer und kann daher auch keine Daten von einem Administrationsagenten annehmen und zu einem späteren Zeitpunkt an den Administrationsserver weiterleiten. Wenn ein Administrationsagent versucht, über das Verbindungs-Gateway eine Verbindung zum Administrationsserver herzustellen, aber das Verbindungs-Gateway keine Verbindung zum Administrationsserver herstellen kann, wird dieses Gateway vom Administrationsagenten als nicht erreichbar angesehen. Alle Daten verbleiben auf dem Administrationsagenten (nicht auf dem Verbindungs-Gateway).

  Ein Verbindungs-Gateway kann keine Verbindung zum Administrationsserver über ein weiteres Verbindungs-Gateway herstellen. Das bedeutet, dass ein Administrationsagent nicht gleichzeitig ein Verbindungs-Gateway sein und ein Verbindungs-Gateway verwenden kann, um eine Verbindung zum Administrationsserver herzustellen.

  Alle Verbindungs-Gateways sind in der Liste der Verteilungspunkte in den Eigenschaften des Administrationsservers enthalten.

- Sie können Verbindungs-Gateways auch innerhalb des Netzwerks verwenden. Beispielsweise werden automatisch zugewiesene Verteilungspunkte auch zu Verbindungs-Gateways in ihrem eigenen Bereich. Innerhalb eines internen Netzwerks bieten Verbindungs-Gateways jedoch keinen wesentlichen Vorteil. Sie reduzieren die Anzahl der vom Administrationsserver empfangenen Netzwerkverbindungen, jedoch nicht das Volumen eingehender Daten. Auch ohne Verbindungs-Gateways können alle Geräte eine Verbindung zum Administrationsserver herstellen.

Hauptinstallationsszenario

Im Anschluss an das dieses Szenario können Sie den Administrationsserver bereitstellen und den Administrationsagenten und Sicherheitsanwendungen auf Geräten im Netzwerk installieren. Sie können dieses Skript verwenden, um sich mit dem Programm vertraut zu machen und das Programm für die weitere Arbeit zu installieren.

Die Installation von Kaspersky Security Center umfasst die folgenden Schritte:

1. Vorbereitende Maßnahmen

2. Installation von Kaspersky Security Center und einer Kaspersky-Sicherheitsanwendung auf dem Administrationsserver-Gerät

3. Zentrale Bereitstellung von Kaspersky-Sicherheitsanwendungen auf den Client-Geräten

Die Bereitstellung von Kaspersky Security Center in einer Cloud-Umgebung sowie die Bereitstellung von Kaspersky Security Center für Dienstanbieter sind in anderen Abschnitten der Hilfe beschrieben.

Wir empfehlen, zur Installation des Administrationsservers mindestens eine Stunde und für die Implementierung des gesamten Szenarios mindestens einen Werktag einzuplanen. Es wird außerdem empfohlen, auf dem Gerät, das als Kaspersky Security Center Administrationsserver dient, eine Sicherheitsanwendung wie Kaspersky Security für Windows Server oder Kaspersky Endpoint Security zu installieren.

Nach der Ausführung aller Schritte des Szenarios wird der Schutz im Unternehmensnetzwerk auf folgende Weise implementiert:

- Das DBMS für den Administrationsserver wird installiert.
- Der Kaspersky Security Center Administrationsserver wird installiert.
- Die erforderlichen Richtlinien und Aufgaben werden erstellt, die Standardeinstellungen der Richtlinien und Aufgaben werden konfiguriert.
- Auf den verwalteten Geräten werden Sicherheitsanwendungen (z. B. Kaspersky Endpoint Security für Windows) und der Administrationsagent installiert.
- Administrationsgruppen werden erstellt (möglichst in einer Hierarchie zusammengefasst).
- Bei Bedarf wird der Schutz mobiler Geräte implementiert.
- Bei Bedarf werden Verteilungspunkte zugewiesen.

Die Installation von Kaspersky Security Center erfolgt in mehreren Schritten:

Vorbereitende Maßnahmen

1. **Abrufen der erforderlichen Dateien**

   Stellen Sie sicher, dass Sie über einen Lizenzschlüssel (Aktivierungscode) für Kaspersky Security Center oder über Lizenzschlüssel (Aktivierungscodes) für Kaspersky-Sicherheitsanwendungen verfügen.

   Entpacken Sie das Archiv, das Sie von Ihrem Vertrieb erhalten haben. Dieses Archiv enthält die Lizenzschlüssel (key-Dateien), die Aktivierungscodes, und eine Liste der Kaspersky-Anwendungen, die mit jedem Lizenzschlüssel aktiviert werden können.

   Wenn Sie Kaspersky Security Center zunächst ausprobieren möchten, können Sie eine kostenlose 30-Tage-Testversion auf der Kaspersky-Website herunterladen.

   Ausführliche Informationen zur Lizenzierung von Kaspersky-Sicherheitsanwendungen, die nicht in Kaspersky Security Center enthalten sind, finden Sie in den Dokumentationen dieser Anwendungen.

2. **Struktur des Schutzes in der Organisation auswählen**

   Machen Sie sich mit den Komponenten von Kaspersky Security Center vertraut. Wählen Sie die Schutzstruktur und die Netzwerkkonfiguration aus, die für Ihre Organisation am besten geeignet sind. Bestimmen Sie ausgehend von der Konfiguration des Netzwerks und der Bandbreite der Übertragungskanäle, wie viele Administrationsserver verwendet und wie sie über die Büros verteilt werden müssen, wenn Sie mit einem verteilten Netzwerk arbeiten.

   Zur Erreichung und Aufrechterhaltung der optimalen Leistung unter verschiedenen Arbeitsbedingungen berücksichtigen Sie die Anzahl der Geräte im Netzwerk, die Netztopologie und den erforderlichen Funktionsumfang von Kaspersky Security Center (Details dazu finden Sie im Handbuch zur Skalierung von Kaspersky Security Center).

   Legen Sie fest, ob eine Hierarchie der Administrationsserver in der Organisation verwendet werden soll. Dazu müssen Sie ermitteln, ob es möglich und sinnvoll ist, alle Client-Geräte mit einem einzigen Administrationsserver zu verwalten, oder ob eine Hierarchie der Administrationsserver aufgebaut werden sollte. Möglicherweise müssen Sie auch eine Hierarchie der Administrationsserver aufbauen, die mit der Organisationsstruktur des Unternehmens übereinstimmt, dessen Netzwerk Sie schützen möchten.

   Wenn Sie den Schutz von mobilen Geräten gewährleisten müssen, konfigurieren Sie als Vorbereitung den iOS MDM-Server.

Stellen Sie sicher, dass die Geräte, die Sie zu Administrationsservern bestimmen möchten, und die Geräte, auf denen die Verwaltungskonsole installiert werden soll, die Hard- und Softwarevoraussetzungen erfüllen.

3. **Vorbereitung der Verwendung benutzerdefinierter Zertifikate**

   Wenn die Public-Key-Infrastruktur (PKI) in Ihrer Organisation die Verwendung von benutzerdefinierten, von einer bestimmten Zertifizierungsstelle (Certification Authority - CA) ausgestellten, Zertifikaten erfordert, bereiten Sie diese Zertifikate vor und stellen Sie sicher, dass sie alle Voraussetzungen erfüllen.

4. **Vorbereitung der Lizenzierung von Kaspersky Security Center**

   Wenn Sie eine Version von Kaspersky Security Center mit Unterstützung der Verwaltung mobiler Geräte, Integration mit SIEM-Systemen und/oder Schwachstellen- und Patch-Management verwenden möchten, stellen Sie sicher, dass Sie über eine Schlüsseldatei oder einen Aktivierungscode für die Programmlizenzierung verfügen.

5. **Vorbereitung der Lizenzierung der verwalteten Sicherheitsanwendungen**

   Während der Bereitstellung des Schutzes werden Sie aufgefordert, Kaspersky aktive Lizenzschlüssel für jene Programme bereitzustellen, die Sie mithilfe von Kaspersky Security Center verwalten möchten (siehe Liste der verwaltbaren Sicherheitsanwendungen). Die Details zur Lizenzierung der einzelnen Sicherheitsanwendungen können Sie in der Dokumentation zu diesen Programmen nachlesen.

6. **Auswahl der Hardwarekonfiguration des Administrationsservers und des DBMS**

   Planen Sie die Hardwarekonfiguration für das DBMS und den Administrationsserver unter Berücksichtigung der Anzahl der Geräte in Ihrem Netzwerk.

7. **Auswahl des DBMS**

   Berücksichtigen Sie bei der DBMS-Auswahl die Anzahl der verwalteten Geräte, die der Administrationsserver abdecken soll. Wenn in Ihrem Netzwerk weniger als 10.000 Geräte vorhanden sind und Sie nicht vorhaben, die Anzahl zu erhöhen, können Sie ein kostenloses Datenbankverwaltungssystem (DBMS) wie SQL Express oder MySQL auswählen und es auf dem Gerät installieren, auf dem sich der Administrationsserver befindet. Alternativ können Sie das MariaDB-DBMS auswählen, mit dem Sie bis zu 20.000 Geräte verwalten können. Wenn in Ihrem Netzwerk mehr als 10.000 Geräte vorhanden sind (oder Sie eine Erweiterung des Netzwerks bis zu einer solchen Geräteanzahl planen), wird empfohlen, ein gebührenpflichtiges SQL-DBMS auszuwählen und auf einem separaten Gerät unterzubringen. Ein gebührenpflichtiges DBMS kann mit mehreren Administrationsservern zusammenarbeiten, ein kostenloses DBMS nur mit einem.

   Wenn Sie SQL Server DBMS auswählen, beachten Sie, dass Sie die in der Datenbank gespeicherten Daten zu MySQL, MariaDB oder Azure-SQL DBMS migrieren können. Um die Migration durchzuführen, sichern Sie Ihre Daten und stellen Sie die Daten im neuen DBMS wieder her.

   > Wenn Sie MSSQL 2019 auswählen, müssen Sie den kumulativen Patch CU12 oder höher verwenden. Dadurch können Sie auftretende Fehler und eine Systemüberlastung vermeiden.

8. **DBMS-Installation und Erstellen der Datenbank**

   Machen Sie sich mit den Benutzerkonten für das Arbeiten mit DBMS vertraut und installieren Sie Ihr DBMS.

   Wählen Sie vor der Installation ein unterstütztes DBMS aus. Sie können beispielsweise PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL oder MariaDB auswählen.

   Informationen zur Installation des ausgewählten DBMS finden Sie in dessen Dokumentation.

   Wenn Sie MariaDB, MySQL, PostgreSQL oder Postgres Pro installieren, verwenden Sie die empfohlenen Einstellungen, um sicherzustellen, dass das DBMS ordnungsgemäß funktioniert.

   Schreiben Sie die Einstellungen des DBMS auf und bewahren Sie diese auf, da sie bei der Installation des Administrationsservers benötigt werden. Diese Einstellungen enthalten den Namen des SQL-Servers, die Portnummer für die Verbindung mit dem SQL-Server, den Benutzerkonto-Namen und das Kennwort für den Zugriff auf den SQL-Server.

Wenn Sie sich entscheiden, PostgreSQL oder Postgres Pro als DBMS zu installieren, stellen Sie sicher, dass Sie ein Kennwort für den Superuser angegeben haben. Wenn das Kennwort nicht angegeben wird, kann sich der Administrationsserver möglicherweise nicht mit der Datenbank verbinden.

Der Installer für Kaspersky Security Center erstellt standardmäßig die Datenbank für die Zuordnung der Informationen des Administrationsservers, Sie können jedoch auf deren Erstellung verzichten und eine andere Datenbank verwenden. Überzeugen Sie sich in diesem Fall davon, dass die Datenbank erstellt wurde, dass Sie ihren Namen kennen und dass dem Benutzerkonto, unter dem der Administrationsservers auf diese Datenbank zugreifen wird, die Rolle db_owner zugewiesen wurde.

Wenden Sie sich erforderlichenfalls an den DBMS-Administrator, falls Sie Informationen benötigen.

9. **Konfiguration der Ports**

   Stellen Sie sicher, dass die Ports geöffnet sind, die für die Interaktion der Komponenten entsprechend der von Ihnen gewählten Schutzstruktur benötigt werden.

   Wenn der Zugriff auf den Administrationsserver aus dem Internet gewährt werden muss, konfigurieren Sie die Ports und die Verbindungseinstellungen je nach Netzwerkkonfiguration.

10. **Überprüfung von Benutzerkonten**

    Überprüfen Sie, ob Sie über lokale Administratorrechte verfügen, damit eine erfolgreiche Installation des Kaspersky Security Center Administrationsservers und die Bereitstellung des Schutzes auf den Geräten gewährleistet ist. Für die Installation des Administrationsagenten auf diesen Geräten sind lokale Administratorrechte auf den Client-Geräten erforderlich. Nach der Installation des Administrationsagenten können Sie mit seiner Hilfe auf dem Gerät eine Remote-Installation von Programmen ohne Benutzerkonto mit Administratorrechten für das Gerät ausführen.

    Der Installer von Kaspersky Security Center installiert auf dem Gerät, das für die Installation des Administrationsservers ausgewählt wurde, standardmäßig drei lokale Benutzerkonten, in deren Namen der Administrationsserver und die Dienste von Kaspersky Security Center gestartet werden:

    - KL-AK-*: Benutzerkonto für Dienst des Administrationsservers.
    - NT Service/KSC*: Benutzerkonto für die übrigen Dienste aus dem Bestand des Administrationsservers.
    - KlPxeUser: Benutzerkonto für die Bereitstellung des Betriebssystems.

    Sie können die Kontoerstellung für die Dienste des Administrationsservers und für andere Dienste deaktivieren. Sie verwenden stattdessen Ihre bereits vorhandenen Benutzerkonten, beispielsweise Domänenbenutzerkonten, wenn Sie vorhaben, den Administrationsserver auf dem Failover-Cluster zu installieren oder aus einem anderen Grund planen, die Domänenbenutzerkonten anstelle der lokalen zu verwenden. Stellen Sie in diesem Fall sicher, dass die zur Ausführung des Administrationsservers und von Kaspersky Security Center vorgesehenen Benutzerkonten erstellt wurden und über alle erforderlichen Berechtigungen zum Zugriff auf das DBMS verfügen (Wenn Sie weiterhin vorhaben, Betriebssysteme über Kaspersky Security Center bereitzustellen, verzichten Sie nicht auf das Erstellen der Benutzerkonten).

Installation von Kaspersky Security Center und einer Kaspersky-Sicherheitsanwendung auf dem Administrationsserver-Gerät

1. **Installation des Administrationsservers, der Verwaltungskonsole, Kaspersky Security Center Web Console und der Verwaltungs-Plug-ins für die Sicherheitsanwendungen**

   Laden Sie Kaspersky Security Center von der Kaspersky-Website herunter. Sie können entweder das vollständige Paket, nur die Web Console oder nur die Verwaltungskonsole herunterladen.

Installieren Sie den Administrationsserver auf dem ausgewählten Gerät (bzw. den Geräten, wenn Sie vorhaben mehr als einen Administrationsserver zu verwenden). Sie können die Standard- oder die benutzerdefinierte Installation des Administrationsservers auswählen. Zusammen mit dem Administrationsserver wird auch die Verwaltungskonsole installiert. Es wird empfohlen, den Administrationsserver anstatt auf einem Domänencontroller auf einem dezidierten Server zu installieren.

Die Standardinstallation wird empfohlen, wenn Sie sich mit Kaspersky Security Center bekannt machen und die Ausführung des Programms z. B. in einem kleinen Bereich des Netzwerks testen möchten. Bei der Standardinstallation passen Sie nur die Einstellungen der Datenbank an. Bei der Standardinstallation konfigurieren Sie nur die Einstellungen der Datenbank und können nur den Standardsatz von Plug-ins zur Verwaltung der Kaspersky-Anwendungen installieren. Sie können die Standardinstallation auch verwenden, wenn Sie bereits Erfahrung mit Kaspersky Security Center haben und in der Lage sind, alle erforderlichen Einstellungen nach der Standardinstallation anzupassen.

Die benutzerdefinierte Installation erlaubt das Ändern bestimmter Einstellungen von Kaspersky Security Center – beispielsweise den Pfad zum freigegebenen Ordner, Benutzerkonten und Ports für die Verbindung mit dem Administrationsserver sowie die Einstellungen der Datenbank. Bei der benutzerdefinierten Installation können Sie angeben, welche Verwaltungs-Plug-ins für Programme von Kaspersky installiert werden sollen. Falls erforderlich, können Sie die benutzerdefinierte Installation im Silent-Modus starten.

Zusammen mit dem Administrationsserver werden auch die Verwaltungskonsole und die Serverversion des Administrationsagenten installiert. Während der Installation können Sie bei Bedarf auch die Kaspersky Security Center Web Console installieren.

Bei Bedarf können Sie die Verwaltungskonsole und/oder die Kaspersky Security Center Web Console separat im Administrator-Arbeitsplatz installieren, um den Administrationsserver über das Netzwerk zu verwalten.

2. **Erstkonfiguration und Lizenzierung**

   Nach Abschluss der Installation des Administrationsservers wird bei der ersten Verbindung mit dem Administrationsserver automatisch der Schnellstartassistent ausgeführt. Befolgen Sie die Schritte des Assistenten, um die Erstkonfiguration des Administrationsservers nach Bedarf vorzunehmen. Während der Erstkonfiguration erstellt der Assistent die zur Bereitstellung des Schutzes notwendigen Richtlinien und Aufgaben mit Standardeinstellungen. Diese Einstellungen sind eventuell nicht optimal für Ihr Unternehmen geeignet. Bei Bedarf können Sie die Einstellungen der Richtlinien und Aufgaben bearbeiten (Schutz im Netzwerk eines Kundenunternehmens anpassen, Szenario: Netzwerkschutz konfigurieren).

   Wenn Sie die Funktionen über die Basisfunktionen hinaus verwenden möchten, lizenzieren Sie die Anwendung. Sie können dies in einem der Schritte des Schnellstartassistenten durchführen.

3. **Überprüfung der erfolgreichen Installation des Administrationsservers**

   Nach der erfolgreichen Ausführung der vorhergehenden Schritte ist der Administrationsserver installiert und zur Verwendung bereit.

   Stellen Sie sicher, dass die Verwaltungskonsole aktiv ist und dass Sie sich mithilfe der Konsole mit dem Administrationsserver verbinden können. Stellen Sie außerdem sicher, dass auf dem Administrationsserver die Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers (im Ordner **Aufgaben** der Konsolenstruktur) und die Richtlinie für Kaspersky Endpoint Security (im Ordner **Richtlinien** der Konsolenstruktur) vorhanden sind.

   Wenn die Prüfung abgeschlossen ist, fahren Sie mit den folgenden Schritten fort.

Zentrale Bereitstellung von Kaspersky-Sicherheitsanwendungen auf den Client-Geräten

1. **Geräte im Netzwerk finden**

   Dieser Schritt ist im Schnellstartassistenten für das Programm vorhanden. Sie können die Gerätesuche auch manuell starten. Daraufhin erhält Kaspersky Security Center die Adressen und die Namen aller Geräte, die im Netzwerk registriert sind. Im Folgenden können Sie mithilfe von Kaspersky Security Center die Anwendungen von Kaspersky und von anderen Herstellern auf den gefundenen Geräten installieren. Da Kaspersky Security Center die Gerätesuche regelmäßig startet, werden neue Geräte im Netzwerk automatisch gefunden, sobald sie auftauchen.

2 Installation des Administrationsagenten und der Sicherheitsanwendungen auf den Geräten im Netzwerk

Als Bereitstellung des Schutzes (Schutz im Netzwerk eines Kundenunternehmens anpassen, Szenario: Netzwerkschutz konfigurieren) im Organisationsnetzwerk wird die Installation des Administrationsagenten sowie einer Sicherheitsanwendung (z. B. Kaspersky Endpoint Security) auf den Geräten verstanden, die vom Administrationsserver bei der Gerätesuche gefunden wurden.

Die Sicherheitsanwendungen schützen Geräte vor Viren und/oder anderen Programmen, die eine Bedrohung darstellen. Der Administrationsagent gewährleistet die Verbindung des Geräts mit dem Administrationsserver. Die Einstellungen des Administrationsagenten werden standardmäßig automatisch angepasst.

Wenn Sie möchten, können Sie den Administrationsagenten im Silent-Modus mit einer Antwortdatei oder ohne eine Antwortdatei installieren.

Bevor Sie den Administrationsagenten und die Sicherheitsanwendungen auf Geräten im Netzwerk installieren, stellen Sie sicher, dass diese Geräte verfügbar (aktiviert) sind. Sie können den Administrationsagenten sowohl auf virtuellen Maschinen als auch auf physischen Geräten installieren.

Die Sicherheitsanwendungen und der Administrationsagent können sowohl per Remote-Installation als auch lokal installiert werden.

Remote-Installation – Sie können mithilfe des Assistenten für die Bereitstellung des Schutzes die Sicherheitsanwendung (z. B. Kaspersky Endpoint Security für Windows) und den Administrationsagenten per Remote-Zugriff auf Geräten installieren, die vom Administrationsserver im Organisationsnetzwerk gefunden wurden. Im Normalfall verteilt die Aufgabe zur Remote-Installation erfolgreich den Schutz für die meisten vernetzten Geräte. Sie kann jedoch auf einigen Geräten einen Fehler zurückgegeben, beispielsweise, wenn ein Gerät ausgeschaltet ist oder aus einem anderen Grund nicht darauf zugegriffen werden kann. In diesem Fall wird empfohlen, eine manuelle Verbindung zum Gerät aufzubauen und eine lokale Installation vorzunehmen.

Lokale Installation – wird auf solchen Geräten im Netzwerk verwendet, auf denen die Verteilung mithilfe der Aufgabe zur Remote-Installation nicht vorgenommen werden konnte. Um den Schutz auf solchen Geräten zu installieren, erstellen Sie ein autonomes Installationspaket für den lokalen Start auf diesen Geräten.

Die Installation des Administrationsagenten auf Geräten mit dem Betriebssystem Linux bzw. macOS, wird in der Dokumentation für Kaspersky Endpoint Security für Linux bzw. für Kaspersky Endpoint Security for Mac beschrieben. Obwohl Geräte mit den Betriebssystemen Linux und macOS als weniger verwundbar gelten als Windows-Geräte, wird empfohlen, Sicherheitsanwendungen auf diesen Geräten zu installieren.

Stellen Sie nach der Installation sicher, dass die Sicherheitsanwendung auf den verwalteten Geräten installiert wurde. Starten Sie dazu den Bericht über die Versionen der Kaspersky-Programme und machen Sie sich mit den Ergebnissen vertraut.

3 Lizenzschlüssel auf Client-Geräte verteilen

Verteilen Sie die Lizenzschlüssel auf die Client-Geräte, um die verwalteten Sicherheitsanwendungen auf diesen Geräten zu aktivieren.

4 Einstellungen zum Schutz mobiler Geräte

Dieser Schritt ist im Schnellstartassistenten für das Programm vorhanden.

Wenn Sie mobile Unternehmensgeräte verwalten möchten, führen Sie die erforderlichen Schritte zur Vorbereitung aus und stellen Sie die Funktion Verwaltung mobiler Geräte bereit.

5 Administrationsgruppenstruktur anlegen

In einigen Fällen müssen für die optimale Implementierung des Schutzes auf den Geräten im Netzwerk die Geräte unter Berücksichtigung der Organisationsstruktur des Unternehmens in Administrationsgruppen zusammengefasst werden. Sie können Verschiebungsregeln für die Verteilung der Geräte auf Gruppen erstellen oder die Geräte manuell verteilen. Für Administrationsgruppen können Gruppenaufgaben und Gültigkeitsbereiche von Richtlinien bestimmt und Verteilungspunkte zugewiesen werden.

Stellen Sie sicher, dass alle verwalteten Geräte den entsprechenden Administrationsgruppen zugewiesen wurden und dass keine nicht zugeordneten Geräte mehr im Netzwerk vorhanden sind.

6 Verteilungspunkte zuweisen

Kaspersky Security Center weist Verteilungspunkte automatisch den Administrationsgruppen zu, aber Sie können diese bei Bedarf auch manuell zuweisen. In den folgenden Fällen wird die Verwendung von Verteilungspunkten empfohlen: In großen Netzwerken, um die Auslastung des Administrationsservers zu senken, sowie in Netzwerken mit einer verteilten Struktur, um dem Administrationsserver Zugriff auf Geräte oder Gerätegruppen zu gewähren, die über Kanäle mit geringer Bandbreite verbunden sind. Sie können neben Windows-Geräten auch Linux-Geräte als Verteilungspunkte einsetzen.

Ports, die von Kaspersky Security Center verwendet werden

Die folgenden Tabellen listen die von den Administrationsservers und Client-Geräten verwendeten Standardports auf. Bei Bedarf können Sie diese standardmäßigen Portnummern ändern.

Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server, Port 1433 für Microsoft SQL Server oder Port 5432 für PostgreSQL und Postgres Pro). Relevante Informationen finden Sie in der DBMS-Dokumentation.

Vom Administrationsserver verwendete Ports

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
8060	klcsweb	TCP	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Sie können die Standard-Portnummer im Abschnitt **Webserver** des Administrationsserver-Eigenschaftenfenster in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern. Dieser Port ist optional. Aus Sicherheitsgründen wird die Verwendung des TCP-Ports 8061 empfohlen.
8061	klcsweb	TCP (TLS)	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Sie können die Standard-Portnummer im Abschnitt **Webserver** des Administrationsserver-Eigenschaftenfenster in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
13000	klserver	TCP (TLS)	Aufnahme der Verbindungen von Administrationsagenten und sekundären Administrationsservern; wird auch auf den sekundären Servern für die Aufnahme der Verbindungen vom primären Administrationsserver verwendet (beispielsweise wenn sich der sekundäre Server in einer DMZ befindet)	Verwaltung von Client-Geräten und sekundären Administrationsservern. Sie können die Nummer des Standardports für den Empfang von Verbindungen von Administrationsagenten ändern, wenn Sie die Verbindungsports konfigurieren. Sie können die Nummer des Standardports für den Empfang von Verbindungen von sekundären Administrationsservern ändern, wenn Sie in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console eine Hierarchie von Administrationsservern erstellen.
13000	klserver	UDP	Annahme der Informationen von Administrationsagenten über das Deaktivieren von Geräten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer in den Richtlinieneinstellungen des Administrationsagenten in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
13291	klserver	TCP (TLS)	Annahme der Verbindungen von der Verwaltungskonsole zum Administrationsserver	Verwaltung des Administrationsservers. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers in der Verwaltungskonsole ändern.

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
13299	klserver	TCP (TLS)	Aufbau von Verbindungen von der Kaspersky Security Center Web Console zum Administrationsserver; Aufbau von Verbindungen mit dem Administrationsserver über OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Sie können die Standard-Portnummer im Eigenschaftenfenster des Administrationsservers ändern (Abschnitt **Verbindungseinstellungen des Administrationsservers** → Unterabschnitt **Verbindungsports**) in der Verwaltungskonsole, oder beim Erstellen einer Hierarchie der Administrationsserver in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console.
14000	klserver	TCP	Annahme der Verbindungen von den Administrationsagenten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer ändern, wenn Sie während der Installation von Kaspersky Security Center die Verbindungsports konfigurieren oder wenn Sie ein Client-Gerät manuell mit dem Administrationsserver verbinden. Dieser Port ist optional. Aus Sicherheitsgründen wird die Verwendung des TCP-Ports 13000 empfohlen.
13111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	TCP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
15111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	UDP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
17000	klactprx	TCP (TLS)	Annahme der Verbindungen von verwalteten Geräten (außer mobile Geräte) zur Anwendungsaktivierung	Aktivierungs-Proxyserver, der von nicht mobilen Geräten verwendet wird, um Kaspersky-Anwendungen mit Aktivierungscodes zu aktivieren. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
17100 (nur wenn Sie mobile Geräte verwalten)	klactprx	TCP (TLS)	Annahme der Verbindungen zur Anwendungsaktivierung auf mobilen Geräten	Proxyserver zur Aktivierung von mobilen Geräten. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
19170	klserver	HTTPS (TLS)	Tunneln der Verbindungen mit verwalteten Geräten mittels "klsctunnel"-Dienstprogramm	Remote-Verbindungen mit verwalteten Geräten herstellen mittels Kaspersky Security Center Web Console. Sie können die standardmäßige Portnummer nur im Eigenschaftenfenster des Administrationsservers in der Verwaltungskonsole ändern (Abschnitt **Verbindungseinstellungen des Administrationsservers** → Unterabschnitt **Verbindungsports** → Option RDP-Port der Kaspersky Security Center Web Console öffnen).
13292 (nur wenn Sie mobile Geräte verwalten)	klserver	TCP (TLS)	Annahme der Verbindungen von mobilen Geräten	Verwaltung mobiler Geräte. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
13294 (nur wenn Sie mobile Geräte verwalten)	klserver	TCP (TLS)	Annahme der Verbindungen von Geräten mit Schutz auf UEFI-Ebene	Verwaltung von Client-Geräten mit Schutz auf UEFI-Ebene. Sie können die standardmäßige Portnummer entweder ändern, wenn Sie mobile Geräte verbinden oder später im Eigenschaftenfenster des Administrationsservers (Abschnitt **Verbindungseinstellungen des Administrationsservers** → Unterabschnitt **Verbindungsports**) in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console.

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
13296	klserver	TCP (TLS)	Veröffentlichen der Metriken von Kaspersky Security Center für Prometheus	Veröffentlichen der Metriken von Kaspersky Security Center, die anschließend von Prometheus abgerufen werden. Sie können die Metriken über folgenden Link anzeigen: https://<Server_Adresse>:13296/metrics. Geben Sie für <Server_Adresse> die IP-Adresse oder den Domänennamen Ihres Administrationsservers an. Sie können die standardmäßige Portnummer in der Verwaltungskonsole im Eigenschaftenfenster des Administrationsservers ändern.
30522, 30523 (Ports der localhost-Schnittstelle)	klnagent	TCP	Abrufen der Anwendungsupdates von Kaspersky für den Administrationsserver über die FileTransferBridge-Komponente	Das Gerät mit dem Administrationsserver, welches Updates für Kaspersky -Anwendungen abruft.

Die folgende Tabelle zeigt den Port, der vom iOS MDM-Server verwendet wird (Nur bei Verwaltung mobiler Geräte).

Port, der vom iOS MDM-Server verwendet wird

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
443	kliosmdmservicesrv	TCP (TLS)	Empfangen von Verbindungen von mobilen iOS-Geräten	Verwaltung mobiler Geräte. Sie können die standardmäßige Portnummer ändern, wenn Sie den iOS MDM-Server installieren.

Die folgende Tabelle zeigt den vom Server der Kaspersky Security Center Web Console verwendeten Port. Es kann sich dabei sowohl um dasselbe Gerät handeln, auf dem der Administrationsserver installiert ist, als auch um ein anderes Gerät.

Port, der vom Server der Web Console von Kaspersky Security Center verwendet wird

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
8080	Node.js: Serverseitiges JavaScript	TCP (TLS)	Empfangen von Verbindungen vom Webbrowser zur Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Sie können die standardmäßige Portnummer ändern, wenn Sie Kaspersky Security Center Web Console auf einem Gerät unter Windows oder auf einer Linux-Plattform installieren. Wenn Sie die Kaspersky Security Center Web Console auf dem ALT Linux-Betriebssystem installieren, müssen Sie eine andere Portnummer als 8080 angeben, da Port 8080 von dem Betriebssystem verwendet wird.

Die folgende Tabelle listet die Ports auf, die von verwalteten Geräten mit installiertem Administrationsagenten verwendet werden.

Ports, die vom Administrationsagenten verwendet werden

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
15000	klnagent	UDP	Verwaltungssignale vom Administrationsserver oder Verwaltungspunkt an die Administrationsagenten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer in den Richtlinieneinstellungen des Administrationsagenten in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
15000	klnagent	UDP-Broadcast	Abrufen von Daten über andere Administrationsagenten in derselben Broadcast-Domäne (die Daten werden dann an den Administrationsserver gesendet)	Zustellung von Updates und Installationspaketen.

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
15001	klnagent	UDP	Empfangen von Multicast-Anfragen von einem Verteilungspunkt (falls verwendet)	Empfang von Updates und Installationspaketen von einem Verteilungspunkt. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunktes in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
30522, 30523 (Ports der localhost-Schnittstelle)	klnagent	TCP	Abrufen der Anwendungsupdates von Kaspersky für den Administrationsserver über die FileTransferBridge-Komponente	Verwaltete Geräte, die Updates für Kaspersky-Anwendungen von einem Administrationsserver abrufen, der als Quelle für das Datenbank-Update angegeben ist.
161	klnagent	SNMP	Überwachung und Erkennung von Netzwerkgeräten.	Auffindbarkeit des Geräts.

Bitte beachten Sie, dass der Prozess "klnagent" auch freie Ports aus dem dynamischen Portbereich eines Endpoint-Betriebssystems anfordern kann. Diese Ports werden dem klnagent-Prozess automatisch vom Betriebssystem zugewiesen, was dazu führen kann, dass der klnagent-Prozess einige Ports verwendet, die von einer anderen Software verwendet werden. Wenn der klnagent-Prozess die Ausführung der Software beeinträchtigt, ändern Sie die Porteinstellungen in dieser Software. Alternativ können Sie den standardmäßigen dynamischen Portbereich in Ihrem Betriebssystem ändern, um den Port auszuschließen, der von der betroffenen Software verwendet wird.

Beachten Sie auch, dass die Empfehlungen zur Kompatibilität von Kaspersky Security Center mit Drittanbieter-Programmen nur referenziellen Charakter besitzen und möglicherweise nicht auf neuere Versionen der Drittanbieter-Programme zutreffen. Die beschriebenen Empfehlungen zur Port-Konfiguration basieren auf den Erfahrungen des Technischen Supports und unseren bewährten Verfahren.

Die nachfolgende Tabelle listet die Ports auf, die von einem verwalteten Gerät mit installiertem Administrationsagenten, welcher als Verteilungspunkt fungiert, verwendet werden. Die aufgelisteten Ports werden von den Verteilungspunkt-Geräten zusätzlich zu den Ports verwendet, die von Administrationsagenten verwendetet werden (siehe Tabelle oben).

Ports, die von einem Administrationsagenten verwendet werden, der als Verteilungspunkt fungiert

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
13000	klnagent	TCP (TLS)	Annehmen der Verbindungen von Administrationsagenten und von Kaspersky Security Center, wenn der Verteilungspunkt als Verbindungs-Gateway in der DMZ agiert Wenn als Verteilungspunkt ein Gerät mit installiertem Administrationsserver angegeben ist, wird für die SSL-Verbindung standardmäßig Port 13001 statt 13000 verwendet.	Verwaltung von Client-Geräten, Zustellung von Updates und Installationspaketen. Weitere Informationen finden Sie in folgenden Thema: Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunktes in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
13111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	TCP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunktes in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
15111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	UDP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunktes in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
17111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	HTTPS	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunktes in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
13295 (nur wenn Sie den Verteilungspunkt als Push-Server verwenden)	klnagent	TCP (TLS)	Annehmen der Verbindungen von Client-Geräten	Push-Server. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunktes in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.

Die folgende Tabelle listet die Ports auf, die vom Gerät eines Domänencontrollers verwendet werden.

Ports, die das Gerät eines Domänencontrollers verwendetet

Portnummer	Protokoll	Zweck des Ports	Gültigkeitsbereich
389	LDAP über TCP oder UDP	Verbindung zu einem LDAP-Server herstellen	Abfrage des Domänencontrollers
636	LDAP über TLS	Verbindung zu einem LDAP-Server herstellen	Abfrage des Domänencontrollers

Die folgende Tabelle enthält den Port, der auf Client-Geräten mit installiertem Administrationsagenten geöffnet sein muss.

Verwendeter Port auf einem nicht zugeordneten Client-Gerät

Portnummer	Protokoll	Zweck des Ports	Gültigkeitsbereich
22	SSH	SSH-Verbindung zu einem Client-Gerät	Nur für Linux-basierte Client-Geräte. Remote-Installation von Kaspersky-Anwendungen über einen Linux-Verteilungspunkt.

Zertifikate für die Ausführung mit Kaspersky Security Center

Dieser Abschnitt enthält Informationen über die Zertifikate von Kaspersky Security Center und beschreibt, wie ein benutzerdefiniertes Zertifikat für den Administrationsserver ausgestellt wird.

Über die Zertifikate von Kaspersky Security Center

Um eine sichere Interaktion zwischen den Komponenten der Anwendung zu ermöglichen, verwendet Kaspersky Security Center die folgenden Arten von Zertifikaten:

- Zertifikat des Administrationsservers
- Mobilgerät-Zertifikat
- Zertifikat des iOS MDM-Servers
- Zertifikat des Kaspersky Security Center Webservers
- Zertifikat der Kaspersky Security Center Web Console

Standardmäßig verwendet Kaspersky Security Center selbstsignierte Zertifikate (d.h., sie werden von Kaspersky Security Center selbst ausgestellt). Sie können diese jedoch durch benutzerdefinierte Zertifikate ersetzen, um den Sicherheitsanforderungen Ihres Unternehmensnetzwerks sowie Sicherheitsstandards besser zu entsprechen. Nachdem der Administrationsserver sichergestellt hat, dass das benutzerdefinierte Zertifikat alle notwendigen Anforderungen erfüllt, nimmt das Zertifikat den gleichen Funktionsumfang wie ein selbstsigniertes Zertifikat an. Der einzige Unterschied besteht darin, dass ein benutzerdefiniertes Zertifikat nach dessen Ablauf nicht automatisch neu ausgestellt wird. Zertifikate können durch benutzerdefinierte Zertifikate ersetzt werden, indem Sie entweder das Dienstprogramm klsetsrvcert verwenden, oder in Abhängigkeit des Zertifikat-Typs den Abschnitt "Eigenschaften des Administrationsservers" in der Verwaltungskonsole verwenden. Wenn Sie das Tool "klsetsrvcert" verwenden, müssen Sie für das Zertifikat einen Typ angeben, indem Sie einen der folgenden Werte verwenden:

- C – gewöhnliches Zertifikat für die Ports 13000 und 13291
- CR – gewöhnliches Reservezertifikat für die Ports 13000 und 13291
- M – Mobilgerät-Zertifikat für den Port 13292
- MR – mobiles Reservezertifikat für den Port 13292
- MCA – mobile Zertifizierungsstelle für automatisch generierte Benutzerzertifikate

> Sie müssen das Dienstprogramm klsetsrvcert nicht herunterladen. Dieses Tool gehört zum Programmpaket von Kaspersky Security Center. Das Tool nicht mit früheren Versionen von Kaspersky Security Center kompatibel.

Die maximale Gültigkeitsdauer für jedes Zertifikat des Administrationsservers beträgt 397 Tage.

Zertifikate des Administrationsservers

Das Zertifikat des Administrationsservers wird zur Authentifizierung des Administrationsservers und zur sicheren Interaktion zwischen dem Administrationsserver und dem Administrationsagenten auf verwalteten Geräten oder zwischen dem primären Administrationsserver und den sekundären Administrationsservern verwendet. Wenn Sie die Verwaltungskonsole mit dem Administrationsserver verbinden, werden Sie dazu aufgefordert, die Verwendung des aktuellen Zertifikats des Administrationsservers zu bestätigen. Außerdem ist eine derartige Bestätigung jedes Mal notwendig, wenn das Zertifikat des Administrationsservers ersetzt wird, wenn der Administrationsserver neu installiert wurde und wenn ein sekundärer Administrationsserver mit dem primären Administrationsserver verbunden wird. Dieses Zertifikat wird als gemeinsames Zertifikat (common - "C") bezeichnet.

Das gemeinsame Zertifikat ("C") wird bei der Installation des Administrationsservers automatisch erstellt. Das Zertifikat besteht aus zwei Teilen:

- Datei "klserver.cer" – befindet sich standardmäßig auf dem Gerät mit installiertem Administrationsserver im Ordner "C:\ProgramData\KasperskyLab\adminkit\1093\cert".

- Geheimer Schlüssel –befindet sich im Windows Protected Storage.

Es existiert außerdem ein gemeinsames Reservezertifikat ("CR"). Kaspersky Security Center generiert dieses Zertifikat 90 Tage vor Ablauf des gemeinsamen Zertifikats automatisch. Das gemeinsame Reservezertifikat wird daraufhin für das nahtlose Ersetzen des Zertifikats des Administrationsservers verwendet. Wenn das gemeinsame Zertifikat im Begriff ist abzulaufen, wird das gemeinsame Reservezertifikat verwendet, um die Verbindung mit den Instanzen der Administrationsagenten auf den verwalteten Geräten aufrecht zu erhalten. Aus diesem Grund wird 24 Stunden vor Ablauf des alten gemeinsame Zertifikates das gemeinsame Reservezertifikat automatisch zum neuen gemeinsamen Zertifikat.

Außerdem können Sie für das Zertifikat des Administrationsservers eine Sicherungskopie, die von anderen Einstellungen des Administrationsservers separiert ist, erstellen, um so den Administrationsserver ohne Datenverlust von einem Gerät auf ein anderes verlegen zu können.

Mobilgerät-Zertifikate

Ein Mobilgerät-Zertifikat (mobile - "M") wird für die Authentifizierung des Administrationsservers auf mobilen Geräten verwendet. Sie können die Verwendung des Mobilgerät-Zertifikat in einem dafür vorgesehenen Schritt des Schnellstartassistenten konfigurieren.

Es existiert außerdem ein Mobilgerät-Reservezertifikat ("MR"): Dieses wird für das nahtlose Ersetzen des Mobilgerät-Zertifikats verwendet. Kaspersky Security Center generiert dieses Zertifikat 60 Tage vor Ablauf des gemeinsamen Zertifikats automatisch. Wenn das Mobilgerät-Zertifikat dabei ist abzulaufen, wird das Mobilgerät-Reservezertifikat verwendet, um die Verbindung mit den Instanzen der Administrationsagenten auf den verwalteten mobilen Geräten aufrecht zu erhalten. Aus diesem Grund wird 24 Stunden vor Ablauf des alten Mobilgerät-Zertifikats das Mobilgerät-Reservezertifikat automatisch zum neuen mobilen Zertifikat.

Wenn Sie für Ihr Verbindungsszenario Client-Zertifikate auf den mobilen Geräten benötigen (für Verbindungen unter Verwendung von Two-Way SSL), können Sie diese Zertifikate unter Verwendung der Zertifizierungsstelle für automatisch generierte Benutzerzertifikate (Mobile Certificate Authority -"MCA") erstellen. Außerdem ermöglicht Ihnen der Schnellstartassistent die umgehende Verwendung von benutzerdefinierten Zertifikaten, die von einer anderen Zertifizierungsstelle ausgestellt wurden, während die Integration mit der Domain Public Key Infrastructure (PKI) Ihrer Organisation es Ihnen ermöglicht, Client-Zertifikate durch Ihre Domain-Zertifizierungsstelle auszustellen.

Zertifikat des iOS MDM-Servers

Das Zertifikat des iOS MDM-Servers wird für die Authentifizierung des Administrationsservers auf mobilen Geräten mit iOS-Betriebssystem benötigt. Die Interaktion mit diesen Geräten wird mittels Apple's Mobile Device Management (MDM)-Protokoll ausgeführt, welches keine Administrationsagenten einbezieht. Stattdessen installieren Sie auf jedem Gerät ein spezielles iOS MDM-Profil, welches ein Client-Zertifikat enthält, um eine Two-Way SSL-Authentifizierung sicherzustellen.

Außerdem ermöglicht Ihnen der Schnellstartassistent die umgehende Verwendung von benutzerdefinierten Zertifikaten, die von einer anderen Zertifizierungsstelle ausgestellt wurden, während die Integration mit der Domain Public Key Infrastructure (PKI) Ihrer Organisation es Ihnen ermöglicht, Client-Zertifikate durch Ihre Domain-Zertifizierungsstelle auszustellen.

Die Client-Zertifikate werden auf iOS-Geräte übertragen, wenn Sie diese iOS MDM-Profile herunterladen. Ein Client-Zertifikat eines iOS MDM-Servers ist für jedes verwaltete iOS-Gerät eindeutig. Sie erstellen alle Client-Zertifikate eines iOS MDM-Servers unter Verwendung der Zertifizierungsstelle für automatisch generierte Benutzerzertifikate (Mobile Certificate Authority -"MCA").

Zertifikat des Kaspersky Security Center Webservers

Der Kaspersky Security Center Webserver (im Folgenden auch "Webserver") ist eine Komponente des Kaspersky Security Center Administrationsservers und verwendet einen speziellen Zertifikatstyp. Dieses Zertifikat wird für die Veröffentlichung von Installationspaketen des Administrationsagenten benötigt, die Sie anschließend auf Ihre verwalteten Geräte herunterladen, sowie für die Veröffentlichung von iOS MDM-Profilen, iOS-Apps und Kaspersky Security for Mobile-Installationspakete. Aus diesem Grund kann der Webserver verschiedene Zertifikate verwenden.

Wenn die Unterstützung von mobilen Geräten deaktiviert ist, verwendet der Webserver eins der folgenden Zertifikate, gegliedert nach Priorität:

1. Benutzerdefiniertes Zertifikat des Webservers, welches Sie manuell in der Verwaltungskonsole angegeben haben
2. Gewöhnliches Zertifikate des Administrationsservers ("C")

Wenn die Unterstützung von mobilen Geräten aktiviert ist, verwendet der Webserver eins der folgenden Zertifikate, gegliedert nach Priorität:

1. Benutzerdefiniertes Zertifikat des Webservers, welches Sie manuell in der Verwaltungskonsole angegeben haben
2. Benutzerdefiniertes Mobilgerät-Zertifikat
3. Selbstsigniertes Mobilgerät-Zertifikat ("M")
4. Gewöhnliches Zertifikate des Administrationsservers ("C")

Zertifikat der Kaspersky Security Center Web Console

Der Server der Web Console von Kaspersky Security Center (im Folgenden als Web Console bezeichnet) verfügt über ein eigenes Zertifikat. Wenn Sie eine Website öffnen, überprüft ein Browser, ob Ihre Verbindung vertrauenswürdig ist. Das Zertifikat der Web Console ermöglicht Ihnen die Authentifizierung der Web Console und wird verwendet, um den Datenverkehr zwischen einem Browser und der Web Console zu verschlüsseln.

Wenn Sie die Web Console öffnen, informiert Sie der Browser möglicherweise darüber, dass die Verbindung zur Web Console nicht privat und das Zertifikat der Web Console ungültig ist. Diese Warnung wird angezeigt, weil das Zertifikat der Web Console selbstsigniert ist und von Kaspersky Security Center automatisch generiert wird. Um diese Warnung zu vermeiden, können Sie Folgendes tun:

- Ersetzen Sie das Zertifikat der Web Console mit einem benutzerdefinierten (empfohlene Option). Erstellen Sie ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt.

- Fügen Sie das Zertifikat der Web Console zur Liste der vertrauenswürdigen Zertifikate des Browsers hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können.

Über das Zertifikat des Administrationsservers

Basierend auf dem *Zertifikat des Administrationsservers* werden zwei Vorgänge durchgeführt: Authentifizierung des Administrationsservers während der Verbindung über die Verwaltungskonsole und Datenaustausch mit den Geräten. Außerdem wird das Zertifikat für die Authentifizierung beim Herstellen einer Verbindung zwischen primären Administrationsservern und sekundären Administrationsservern verwendet.

Zertifikat ausgestellt von Kaspersky

Das Zertifikat des Administrationsservers wird bei der Installation der Komponente "Administrationsserver" automatisch angelegt und im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert gespeichert.

Das Zertifikat des Administrationsservers ist fünf Jahre lang gültig, wenn das Zertifikat mit einem Administrationsserver in den Versionen 12.2 oder früher erstellt wurde. Andernfalls ist der Gültigkeitszeitraum des Zertifikats auf 397 Tage begrenzt. Ein neues Zertifikat wird vom Administrationsserver als Reservezertifikat 90 Tage vor dem Ablaufdatum des aktuellen Zertifikats generiert. Das neue Zertifikat ersetzt das aktuelle Zertifikat automatisch einen Tag vor dem Ablaufdatum. Alle Administrationsagenten auf den Client-Geräten werden automatisch neu konfiguriert, um den Administrationsserver mit dem neuen Zertifikat zu authentifizieren.

Benutzerdefinierte Zertifikate

Bei Bedarf können Sie dem Administrationsserver ein benutzerdefiniertes Zertifikat zuweisen. Dies kann beispielsweise für eine bessere Integration in die vorhandene PKI Ihres Unternehmens oder für die benutzerdefinierte Konfiguration der Zertifikatfelder erforderlich sein.

Die maximale Gültigkeitsdauer für jedes Zertifikat des Administrationsservers beträgt 397 Tage.

Beim Ersetzen des Zertifikates stellen alle Administrationsagenten, die zuvor mittels SSL mit Administrationsserver verbunden waren, keine Verbindung mit dem Server mehr her und geben den Fehler "Fehler bei der Authentifizierung des Administrationsservers" zurück. Um diesen Fehler zu beheben, müssen Sie die Verbindung nach dem Ersetzen des Zertifikats wiederherstellen.

Sollte das Zertifikat des Administrationsservers verloren gehen, sind zu dessen Wiederherstellung eine Neuinstallation der Komponente "Administrationsserver" und eine anschließende Wiederherstellung der Daten erforderlich.

Wenn Sie Kaspersky Security Center Web Console in verschiedenen Browsern öffnen und im Eigenschaftenfenster des Administrationsservers die Datei mit dem Zertifikat des Administrationsservers herunterladen, haben die Dateien unterschiedliche Namen.

Anforderungen an benutzerdefinierte Zertifikate für deren Verwendung in Kaspersky Security Center

Die unten stehende Tabelle zeigt die Voraussetzungen für benutzerdefinierte Zertifikate, angegeben in Bezug auf verschiedene Komponenten von Kaspersky Security Center, an.

Voraussetzungen für Zertifikate von Kaspersky Security Center

Typ des Zertifikats	Voraussetzungen	Kommentare
Gewöhnliches Zertifikat, gewöhnliches Reservezertifikat ("C", "CR")	Minimale Schlüssellänge: 2048 Basic constraints: • Path Length Constraint: None Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (optional): Serverauthentifizierung, Clientauthentifizierung Das Zertifikat muss einen gültigen "Subject Alternative Name" (SAN) enthalten, der die Loopback-Adresse des Administrationsservers enthält: • Für IPv4: 127.0.0.1 • Für IPv6: 0:0:0:0:0:0:0:1	Der Parameter für Extended Key Usage ist optional. Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, aber darf nicht kleiner als "1" sein.
Mobilgerät-Zertifikat, Mobilgerät-Reservezertifikat ("M", "MR")	Minimale Schlüssellänge: 2048 Basic constraints: • CA: true • Path Length Constraint: None Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (optional): Serverauthentifizierung.	Der Parameter für Extended Key Usage ist optional. Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, wenn der Wert von Path Length Constraint des Common Certificates nicht kleiner als "1" ist.
CA-Zertifikat für automatisch generierte Benutzerzertifikate ("MCA")	Minimale Schlüssellänge: 2048 Basic constraints: • CA: true • Path Length Constraint: None Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (optional): Serverauthentifizierung, Clientauthentifizierung	Der Parameter für Extended Key Usage ist optional. Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, wenn der Wert von Path Length Constraint des Common Certificates nicht kleiner als "1" ist.

Typ des Zertifikats	Voraussetzungen	Kommentare
Zertifikat des Webservers	Extended Key Usage: Serverauthentifizierung Der PKCS #12- / PEM-Container, aus dem das Zertifikat angegeben wird, enthält die vollständige Kette der öffentlichen Schlüssel. Der "Subject Alternative Name" (SAN) des Zertifikats ist vorhanden. Das heißt, dass der Wert des Feldes `subjectAltName` zulässig ist. Das Zertifikat erfüllt die aktuell wirksamen Anforderungen des Browsers an Serverzertifikate, sowie die aktuell gültigen Grundvoraussetzungen des CA/Browser Forums.	—
Zertifikat der Kaspersky Security Center Web Console	Der PEM-Container, aus dem das Zertifikat angegeben wird, enthält die vollständige Kette der öffentlichen Schlüssel. Der "Subject Alternative Name" (SAN) des Zertifikats ist vorhanden. Das heißt, dass der Wert des Feldes `subjectAltName` zulässig ist. Das Zertifikat erfüllt die aktuell wirksamen Anforderungen des Browsers an Serverzertifikate, sowie die aktuell gültigen Grundvoraussetzungen des CA/Browser Forums.	Verschlüsselte Zertifikate werden von Kaspersky Security Center Web Console nicht unterstützt.

Szenario: Angeben des benutzerdefinierten Zertifikats des Administrationsservers

Sie können das benutzerdefinierte Zertifikat des Administrationsservers beispielsweise für eine bessere Integration in die vorhandene Public-Key-Infrastruktur (PKI) Ihres Unternehmens oder für eine benutzerdefinierte Konfiguration der Zertifikatfelder angeben. Es ist zweckmäßig, das Zertifikat sofort nach der Installation des Administrationsservers vor dem Abschluss des Schnellstartassistenten zu ersetzen.

Die maximale Gültigkeitsdauer für jedes Zertifikat des Administrationsservers beträgt 397 Tage.

Erforderliche Vorrausetzungen

Dabei müssen die folgende Bedingungen erfüllt sein:

- Das neue Zertifikat muss im PKCS#12-Format erstellt werden (z. B. unter Verwendung der PKI des Unternehmens).
- Für das neue Zertifikat müssen die in der folgenden Tabelle aufgeführten Voraussetzungen erfüllt sein.

  Beachten Sie in der folgenden Tabelle die Anforderung "CA: true", die angibt, dass das neue Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority – CA) ausgestellt sein muss. Das neue Zertifikat mit der Anforderung "CA: true" muss die gesamte Vertrauenskette und einen privaten Schlüssel enthalten, welcher in einer Datei mit pfx- oder p12-Erweiterung gespeichert werden muss.

Voraussetzungen für die Zertifikate des Administrationsservers

Typ des Zertifikats	Voraussetzungen
Gewöhnliches Zertifikat, gewöhnliches Reservezertifikat ("C", "CR")	Minimale Schlüssellänge: 2048 Basic constraints: • Path Length Constraint: None Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, aber darf nicht kleiner als "1" sein. Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (EKU): Serverauthentifizierung und Clientauthentifizierung. Die EKU ist optional, aber wenn Ihr Zertifikat diese enthält, müssen die Authentifizierungsdaten für Server und Client in der EKU angegeben werden. Das Zertifikat muss einen gültigen "Subject Alternative Name" (SAN) enthalten. Das Feld `subjectAltName` muss die Loopback-Adresse des Administrationsservers enthalten: • Für IPv4: 127.0.0.1 • Für IPv6: 0:0:0:0:0:0:0:1
Mobilgerät-Zertifikat, Mobilgerät-Reservezertifikat ("M", "MR")	Minimale Schlüssellänge: 2048 Basic constraints: • CA: true • Path Length Constraint: None Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, wenn der Wert von Path Length Constraint des Common Certificates nicht kleiner als "1" ist. Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (EKU): Serverauthentifizierung. Die EKU ist optional, aber wenn Ihr Zertifikat diese enthält, müssen die Authentifizierungsdaten des Servers in der EKU angegeben werden.
CA-Zertifikat für automatisch generierte Benutzerzertifikate ("MCA")	Minimale Schlüssellänge: 2048 Basic constraints: • CA: true • Path Length Constraint: None Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, wenn der Wert von Path Length Constraint des Common Certificates nicht kleiner als "1" ist. Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (EKU): Clientauthentifizierung. Die EKU ist optional, aber wenn Ihr Zertifikat diese enthält, müssen die Authentifizierungsdaten des Clients in der EKU angegeben werden.

Von einer öffentlichen Zertifizierungsstelle ausgestellte Zertifikate verfügen nicht über die Berechtigung zum Signieren von Zertifikaten. Um solche Zertifikate zu verwenden, stellen Sie sicher, dass Sie den Administrationsagenten ab Version 13 auf den Verteilungspunkten oder Verbindungsgateways in Ihrem Netzwerk installiert haben. Andernfalls können Sie Zertifikate ohne die Berechtigung zum Signieren nicht verwenden.

Schritte

Das Angeben des Zertifikats des Administrationsservers erfolgt schrittweise:

1. **Ersetzen des Zertifikat des Administrationsservers**

   Verwenden Sie dafür das Befehlszeilendienstprogramm klsetsrvcert.

2. **Angeben eines neuen Zertifikats und Wiederherstellen der Verbindung der Administrationsagenten zum Administrationsserver**

   Wenn das Zertifikat ersetzt wird, verlieren alle Administrationsagenten, die zuvor mittels SSL mit Administrationsserver verbunden waren, die Verbindung zum Server und geben den Fehler "Fehler bei der Authentifizierung des Administrationsservers" zurück. Verwenden Sie das Befehlszeilendienstprogramm klmover, um das neue Zertifikat zu spezifizieren und die Verbindung wiederherzustellen.

3. **Angeben eines neuen Zertifikats in den Einstellungen der Kaspersky Security Center Web Console**

   Nachdem Sie das Zertifikat ersetzt haben, müssen Sie es in den Einstellungen der Kaspersky Security Center Web Console angeben. Andernfalls kann die Kaspersky Security Center Web Console keine Verbindung zum Administrationsserver herstellen.

Ergebnisse

Wenn Sie das Szenario abgeschlossen haben, wurde das Zertifikat des Administrationsservers ersetzt und der Server wurde durch Administrationsagenten auf den Client-Geräten authentifiziert.

Zertifikats des Administrationsservers mittels Tool "klsetsrvcert" ersetzen

So ersetzen Sie das Zertifikat des Administrationsservers:

Führen Sie aus der Befehlszeile das folgenden Dienstprogramm aus:

```
klsetsrvcert [-t <Zertifikat-Typ> {-i <Pfad zum neuen Zertifikat> [-p <Kennwort>] [-o
<Parameter>] | -g <DNS-Name>}][-f <Zeitpunkt der Ersetzung>][-r <Root-Zertifikate>][-l
<Pfad zur Protokolldatei>]
```

Sie müssen das Dienstprogramm klsetsrvcert nicht herunterladen. Dieses Tool gehört zum Programmpaket von Kaspersky Security Center. Es ist nicht mit früheren Versionen von Kaspersky Security Center kompatibel.

Die Beschreibung der Parameter des Dienstprogramms klsetsrvcert finden Sie in der folgenden Tabelle.

Parameterwerte des Dienstprogramms klsetsrvcert

Parameter	Wert
`-t < Zertifikat-Typ >`	Typ des Zertifikats, das ersetzt werden muss. Mögliche Einstellungswerte des Parameters `< Zertifikat-Typ >`: • `C` – gewöhnliches Zertifikat für die Ports 13000 und 13291 ersetzen. • `CR` – gewöhnliches Reservezertifikat für die Ports 13000 und 13291 ersetzen. • `M` – Zertifikat für mobile Geräte für den Port 13292 ersetzen. • `MR` – mobiles Reservezertifikat für den Port 13292 ersetzen. • `MCA` – mobile Client-Zertifizierungsstelle für automatisch generierte Benutzerzertifikate.

Parameter	Wert
`-f <Zeitpunkt des Ersetzens>`	Zeitplan für das Ersetzen der Zertifikate im Format "DD-MM-YYYY hh:mm" (für die Ports 13000 und 13291). Verwenden Sie diesen Parameter, wenn Sie das gemeinsame Zertifikat mit dem Reservezertifikat ersetzen möchten, bevor das gemeinsame Zertifikat abläuft. Geben Sie die Zeit an, zu der verwaltete Geräte mit dem Administrationsserver mit einem neuen Zertifikat synchronisiert werden müssen.
`-i <Pfad zum neuen Zertifikat>`	Container mit dem Zertifikat und privatem Schlüssel im Format PKCS#12 (Datei mit der p12- oder pfx-Erweiterung).
`-p <Kennwort>`	Kennwort, mithilfe dessen der p12-Container geschützt ist. Da das Zertifikat und ein privater Schlüssel im Container gespeichert werden, wird das Kennwort benötigt, um die Datei mit dem Container zu entschlüsseln.
`-o <Validierungsparameter>`	Parameter der Zertifikatsvalidierung (durch Strichpunkt getrennt). Um ein benutzerdefiniertes Zertifikat ohne Signaturberechtigung zu verwenden, geben Sie im Dienstprogramm klsetsrvcert `-o NoCA` an. Dies ist nützlich für Zertifikate, die von einer öffentlichen Zertifizierungsstelle ausgestellt wurden. Um für Zertifikate vom Typ C oder CR die Länge des Chiffrierschlüssels zu ändern, geben Sie in dem Tool "klsetsrvcert" die Option `-o RsaKeyLen:<Schlüssellänge>` an, wobei der Parameter `<Schlüssellänge>` der erforderlichen Länge des Schlüssels entspricht. Andernfalls wird die aktuelle Länge des Zertifikatsschlüssels verwendet.
`-g <DNS-Name>`	Ein neues Zertifikat wird für den angegebenen DNS-Namen erstellt.
`-r <Root-Zertifikate>`	Liste mit vertrauenswürdigen Zertifizierungsstellen für Stammzertifikate im Format PEM.
`-l <Pfad zur Protokolldatei>`	Datei zur Ausgabe der Ergebnisse. Standardmäßig erfolgt die Ausgabe im Standardausgabestream.

Um das benutzerdefinierte Zertifikat des Administrationsservers anzugeben, verwenden Sie beispielsweise den folgenden Befehl:

```
klsetsrvcert -t C -i <Pfad zum neuen Zertifikat> -p <Kennwort> -o NoCA
```

Nachdem das Zertifikat ersetzt wurde, verlieren alle Administrationsagenten, die über SSL mit dem Administrationsserver verbunden sind, ihre Verbindung. Verwenden Sie das Befehlszeilen-Dienstprogramm klmover, um es Wiederherstellen.

Um zu vermeiden, dass die Verbindungen mit den Administrationsagenten verloren gehen, verwenden Sie die folgenden Befehle:

1. Um ein neues Zertifikats zu installieren:

   ```
   klsetsrvcert.exe -t CR -i <Pfad zum neuen Zertifikat> -p <kennwort> -o NoCA
   ```

2. Um ein Datum anzugeben, an dem das Zertifikat angewendet wird:

   ```
   klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
   ```

Wobei `DD-MM-YYYY hh:mm` das Datum 3-4 Wochen nach dem aktuellen Datum darstellt. Der zeitliche Versatz ist zum Austauschen des Zertifikats durch ein neues vorgesehen und ermöglicht die Verteilung dieses neuen Zertifikats an alle Administrationsagenten.

Administrationsagenten mit dem Administrationsserver mittels Dienstprogramm klmover verbinden

Nachdem Sie das Zertifikat des Administrationsservers mit dem Dienstprogramm klsetsrvcert über die Befehlszeile ersetzt haben, müssen Sie die SSL-Verbindung zwischen den Administrationsagenten und dem Administrationsserver herstellen, da die Verbindung unterbrochen wurde.

So geben Sie das neue Zertifikat des Administrationsservers an und stellen die Verbindung wieder her:

Führen Sie aus der Befehlszeile das folgenden Dienstprogramm aus:

```
klmover [-address <Server-Adresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatdatei>]
```

Zum Ausführen des Tools sind Administratorrechte erforderlich.

Das Dienstprogramm wird automatisch in den Installationsordner des Administrationsagenten kopiert, wenn der Administrationsagent auf einem Client-Gerät installiert wird.

Um zu verhindern, dass Angreifer Geräte aus dem Kontrollbereich Ihres Administrationsservers heraus verschieben können, wird es dringend empfohlen, für die Ausführung des Tools "klmover" den Kennwortschutz zu aktivieren. Um den Kennwortschutz zu aktivieren, wählen Sie in den Richtlinieneinstellungen des Administrationsagenten die Option **Deinstallationskennwort verwenden**.

Das Tool "klmover" erfordert lokale Administratorrechte. Für Geräte, die ohne lokale Administratorrechte betrieben werden, kann der Kennwortschutz für die Ausführung des Tools "klmover" ausgelassen werden.

Das Aktivieren der Option **Deinstallationskennwort verwenden** aktiviert ebenfalls den Kennwortschutz für das Cleaner-Tool (cleaner.exe).

Sie können das Tool "klmover" nicht für Client-Geräte verwenden, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind. Für solche Geräte müssen Sie entweder den Administrationsagenten neu konfigurieren oder den Administrationsagenten neu installieren und das Verbindungs-Gateway angeben.

Die Beschreibung der Parameter des Dienstprogramms klmover finden Sie in der folgenden Tabelle.

Parameterwerte des Dienstprogramms klmover

Parameter	Wert
`-address <Serveradresse>`	Adresse des Administrationsservers für die Verbindung. Es kann die IP-Adresse, der NetBIOS-Name oder der DNS-Name angegeben werden.
`-pn <Portnummer>`	Nummer des Ports, über den eine ungesicherte Verbindung zum Administrationsserver hergestellt wird. Standardmäßig wird Portnummer 14000 verwendet.
`-ps <SSL-Portnummer>`	Nummer des SSL-Ports, über den eine gesicherte Verbindung zum Administrationsserver mit dem SSL-Protokoll hergestellt wird. Standardmäßig wird Portnummer 13000 verwendet.
`-nossl`	Ungesicherte Verbindung zum Administrationsserver verwenden. Wenn kein Schlüssel verwendet wird, erfolgt die Verbindung des Administrationsagenten mit dem Administrationsserver über das SSL-Protokoll.

Parameter	Wert
`-cert < Pfad zur Zertifikatsdatei >`	Angegebene Zertifikatsdatei für Authentifizierung am Administrationsserver verwenden.
`-virtserv`	Name des virtuellen Administrationsservers.
`-cloningmode`	Modus des Administrationsagenten zum Klonen von Laufwerken. Verwenden Sie einen der folgenden Parameter, um den Modus zum Klonen von Laufwerken zu konfigurieren: • `-cloningmode` – Status des Modus zum Klonen von Laufwerken abfragen. • `-cloningmode 1` – Modus zum Klonen von Laufwerken aktivieren. • `-cloningmode 0` – Modus zum Klonen von Laufwerken deaktivieren.
`-nauninstpwd < Kennwort >`	Verwenden Sie diesen Parameter, um das Kennwort für die Deinstallation des Administrationsagenten anzugeben. Der Parameter ist nicht obligatorisch.

Um beispielsweise den Administrationsagenten mit dem Administrationsserver zu verbinden, führen Sie den folgenden Befehl aus:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Neuausstellung des Webserver-Zertifikats

Das in Kaspersky Security Center verwendete Zertifikat des Webservers wird für die Veröffentlichung von Installationspaketen des Administrationsagenten, die Sie anschließend auf Ihre verwalteten Geräte herunterladen, genauso benötigt, wie für die Veröffentlichung von iOS MDM-Profilen, iOS-Apps und Installationspaketen von Kaspersky Endpoint Security for Mobile. Abhängig von der aktuellen Programmkonfiguration können verschiedene Zertifikate als Webserver-Zertifikat fungieren (weitere Informationen finden Sie unter Informationen zu Kaspersky Security Center-Zertifikaten).

Möglicherweise müssen Sie das Webserver-Zertifikat erneut ausstellen, um die spezifischen Sicherheitsanforderungen Ihres Unternehmens zu erfüllen oder die kontinuierliche Verbindung Ihrer verwalteten Geräte aufrechtzuerhalten, bevor Sie mit dem Upgrade des Programms beginnen. Kaspersky Security Center bietet zwei Möglichkeiten, das Webserver-Zertifikat erneut auszustellen. Die Wahl zwischen den beiden Methoden hängt davon ab, ob Sie mobile Geräte über das mobile Protokoll verbunden und verwaltet haben (d. h. mithilfe des Mobilgerät-Zertifikats).

Wenn Sie im Abschnitt **Webserver** des Eigenschaftenfensters des Administrationsservers noch nie ein eigenes benutzerdefiniertes Zertifikat als Webserver-Zertifikat angegeben haben, fungiert das Mobilgerät-Zertifikat als Webserver-Zertifikat. In diesem Fall wird die Neuausstellung des Webserver-Zertifikats durch die Neuausstellung des mobilen Protokolls selbst durchgeführt.

So stellen Sie das Webserver-Zertifikat erneut aus, wenn Sie keine mobilen Geräte über das mobile Protokoll verwaltet haben:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Namen des Administrationsservers und wählen Sie im Kontextmenü **Eigenschaften** aus.

2. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers auf der linken Seite den Abschnitt **Verbindungseinstellungen des Administrationsservers** aus.

3. In der Liste der Unterabschnitte wählen Sie den Unterabschnitt **Zertifikate** aus.

4. Wenn Sie das von Kaspersky Security Center ausgestellte Zertifikat weiterhin verwenden möchten, gehen Sie wie folgt vor:

   a. Wählen Sie im rechten Bereich in der Gruppe **Authentifizierung des Administrationsservers durch mobile Geräte** der Einstellungen die Option **Das Zertifikat wurde mithilfe des Administrationsservers ausgestellt** aus und klicken Sie auf die Schaltfläche **Neu ausstellen**.

   b. Wählen Sie im folgenden Fenster **Zertifikat erneut ausstellen** in der Gruppe der Einstellungen **Adresse der Verbindung** und **Aktivierungsfrist** die entsprechenden Optionen aus und klicken Sie auf **OK**.

   c. Klicken Sie im Bestätigungsfenster auf **Ja**.

   Wenn Sie alternativ Ihr eigenes benutzerdefiniertes Zertifikat verwenden möchten, gehen Sie wie folgt vor:

   a. Prüfen Sie, ob Ihr benutzerdefiniertes Zertifikat die Anforderungen von Kaspersky Security Center erfüllt. Ändern Sie das Zertifikat bei Bedarf.

   b. Aktivieren Sie die Option **Anderes Zertifikat** und klicken Sie auf die Schaltfläche **Durchsuchen**.

   c. Wählen Sie im folgenden Fenster **Zertifikat** im Feld **Zertifikatstyp** den Typ Ihres Zertifikats aus und geben Sie den Speicherort und die Einstellungen des Zertifikats an:

      - Wenn Sie **Container PKCS#12** ausgewählt haben, klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Zertifikatdatei** und geben Sie die Zertifikatdatei auf Ihrer Festplatte an. Wenn die Zertifikatdatei kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort (falls vorhanden)** ein.

      - Wenn Sie **X.509-Zertifikat** ausgewählt haben, klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Privater Schlüssel (.prk, .pem)** und geben Sie den privaten Schlüssel auf Ihrer Festplatte an. Wenn der private Schlüssel kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort (falls vorhanden)** ein. Klicken Sie dann auf die Schaltfläche **Durchsuchen** neben dem Feld **Offener Schlüssel (.cer)** und geben Sie den privaten Schlüssel auf Ihrer Festplatte an.

   d. Klicken Sie im Fenster **Zertifikat** auf **OK**.

   e. Klicken Sie im Bestätigungsfenster auf **Ja**.

   Das Mobilgerät-Zertifikat wird erneut ausgestellt, um als Webserver-Zertifikat verwendet zu werden.

So stellen Sie das Webserver-Zertifikat erneut aus, wenn Sie keine mobilen Geräte über das mobile Protokoll verwalten:

1. Generieren Sie Ihr benutzerdefiniertes Zertifikat und bereiten Sie es für die Verwendung im Kaspersky Security Center vor. Prüfen Sie, ob Ihr benutzerdefiniertes Zertifikat die Anforderungen von Kaspersky Security Center erfüllt. Ändern Sie das Zertifikat bei Bedarf.

2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Namen des Administrationsservers und wählen Sie im Kontextmenü **Eigenschaften** aus.

3. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers auf der linken Seite den Abschnitt **Webserver** aus.

4. Wählen Sie im Menü **Über HTTPS-Protokoll** die Option **Anderes Zertifikat angeben**.

5. Klicken Sie im Menü **Über HTTPS-Protokoll** auf die Schaltfläche **Ändern**.

6. Wählen Sie im folgenden Fenster **Zertifikat** im Feld **Zertifikatstyp** den Typ Ihres Zertifikats aus:

   - Wenn Sie **Container PKCS#12** ausgewählt haben, klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Zertifikatdatei** und geben Sie die Zertifikatdatei auf Ihrer Festplatte an. Wenn die Zertifikatdatei kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort (falls vorhanden)** ein.

   - Wenn Sie **X.509-Zertifikat** ausgewählt haben, klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Privater Schlüssel (.prk, .pem)** und geben Sie den privaten Schlüssel auf Ihrer Festplatte an. Wenn der private Schlüssel kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort (falls vorhanden)** ein. Klicken Sie dann auf die Schaltfläche **Durchsuchen** neben dem Feld **Offener Schlüssel (.cer)** und geben Sie den privaten Schlüssel auf Ihrer Festplatte an.

7. Klicken Sie im Fenster **Zertifikat** auf **OK**.

8. Ändern Sie bei Bedarf im Eigenschaftenfenster des Administrationsservers im Feld **Webserver-HTTPS-Port** die Nummer des HTTPS-Ports für den Webserver. Klicken Sie auf die Schaltfläche **OK**.

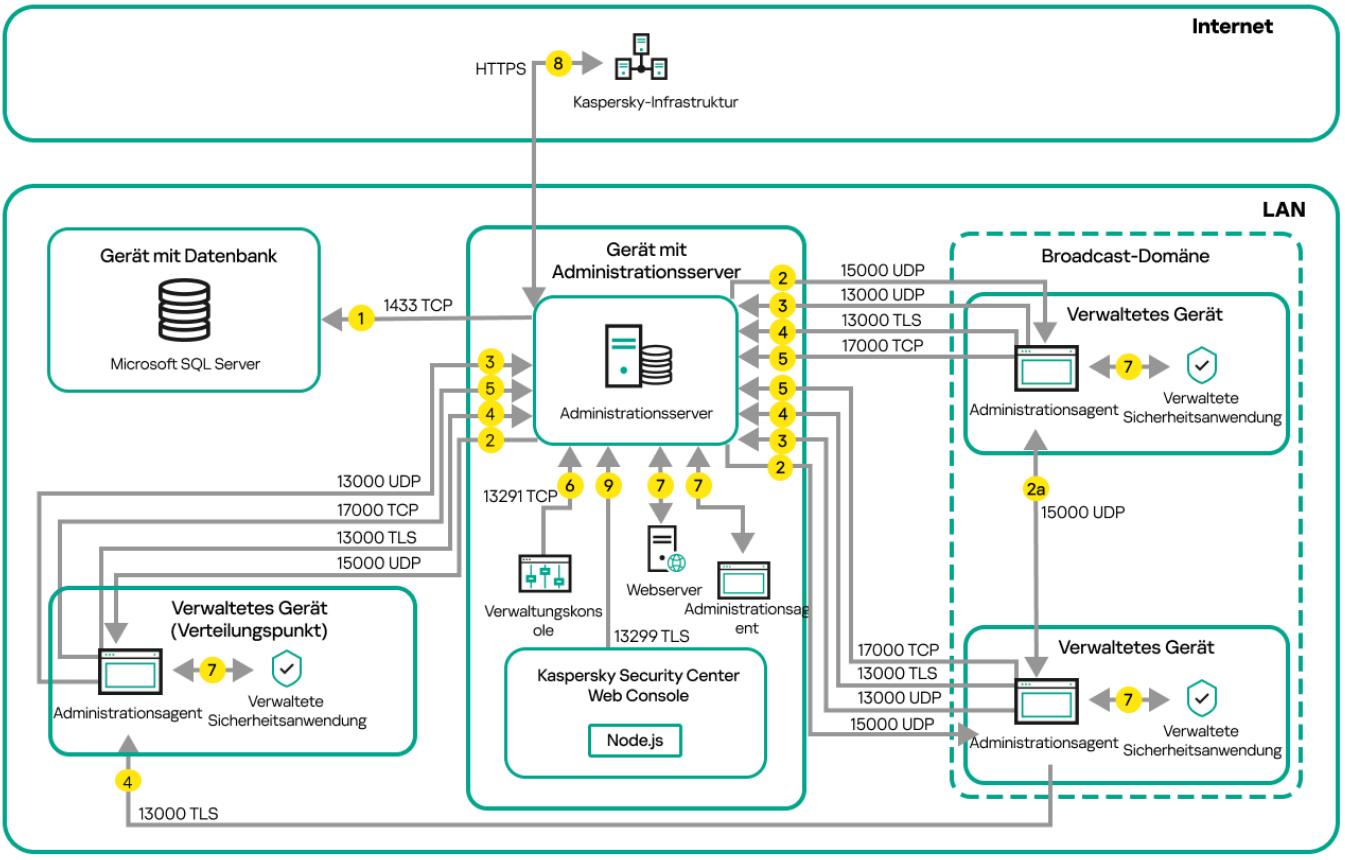
   Das Webserver-Zertifikat wird erneut ausgestellt.

Schemata für Datenverkehr und Portnutzung

Dieser Abschnitt enthält Schemata für den Datenverkehr zwischen den Komponenten von Kaspersky Security Center, den verwalteten Sicherheitsanwendungen und den externen Servern unter Berücksichtigung unterschiedlicher Konfigurationen. Die Schemata geben an, welche Ports auf den lokalen Geräten verfügbar sein müssen.

Administrationsserver und verwaltete Geräte im LAN

Die folgende Abbildung zeigt den Datenverkehr bei einer Verteilung von Kaspersky Security Center ausschließlich im lokalen Netzwerk (LAN).



Administrationsserver und verwaltete Geräte im lokalen Netzwerk (LAN)

Die Abbildung zeigt, wie verschiedene verwaltete Geräte auf unterschiedliche Arten mit dem Administrationsserver verbunden sind: Direkt oder über einen Verteilungspunkt. Verteilungspunkte verringern die Belastung auf dem Administrationsserver während der Update-Verteilung und optimieren den Netzwerkdatenverkehr. Verteilungspunkte werden jedoch nur benötigt, wenn die Anzahl an verwalteten Geräten entsprechend groß ist. Bei einer geringen Anzahl an verwalteten Geräten können alle Geräte die Updates direkt vom Administrationsserver empfangen.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, dass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server, oder Port 1433 für Microsoft SQL Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den TLS-Port 13000 zu verwenden.

   > Der Verteilungspunkt wurde in früheren Versionen von Kaspersky Security Center "Update-Agent" genannt.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Die Daten der MMC-basierten Verwaltungskonsole werden über Port 13291 an den Administrationsserver übertragen (Der Administrationsserver kann auf dem gleichen oder einem anderen Gerät installiert sein).

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

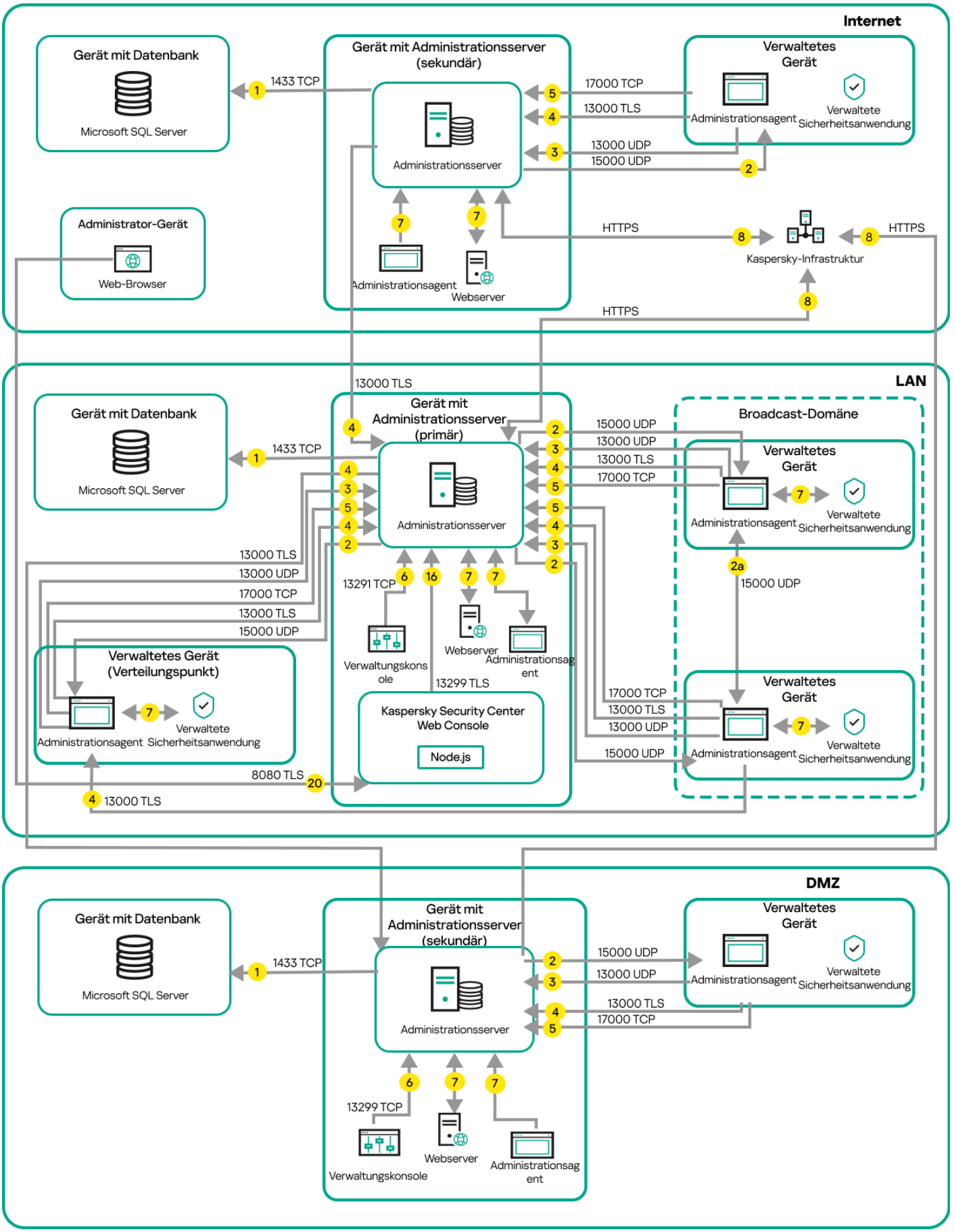
8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

Primärer Administrationsserver im LAN und zwei sekundäre Administrationsserver

Die folgende Abbildung zeigt die Hierarchie der Administrationsserver an: der primäre Administrationsserver befindet sich im lokalen Netzwerk (LAN). Ein sekundärer Administrationsserver befindet sich in der demilitarisierten Zone (DMZ) und ein weiterer sekundärer Administrationsserver im Internet.



Hierarchie der Administrationsserver: primärer Administrationsserver und zwei sekundäre Administrationsserver

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, dass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server, oder Port 1433 für Microsoft SQL Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den TLS-Port 13000 zu verwenden.

   > Der Verteilungspunkt wurde in früheren Versionen von Kaspersky Security Center "Update-Agent" genannt.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Die Daten der MMC-basierten Verwaltungskonsole werden über Port 13291 an den Administrationsserver übertragen (Der Administrationsserver kann auf dem gleichen oder einem anderen Gerät installiert sein).

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

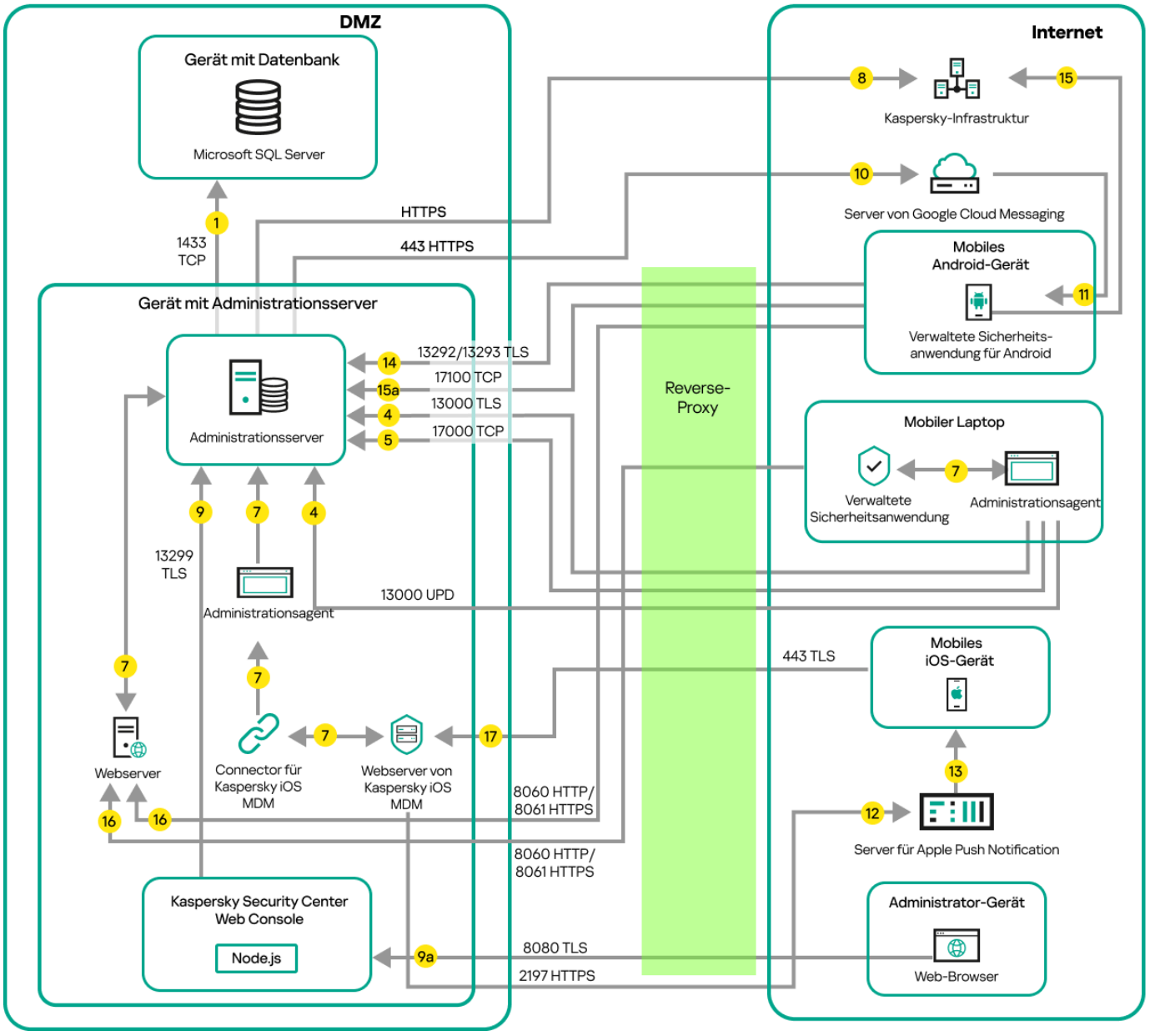
   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   9a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Kaspersky Security Center Web Console kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

Administrationsserver im LAN, verwaltete Geräte im Internet und Verwendung eines Reverse-Proxys

Die folgende Abbildung zeigt den Datenverkehr für das Szenario, bei dem sich der Administrationsserver im lokalen Netzwerk (LAN) befindet, während sich die verwalteten Geräte – einschließlich mobiler Geräte – im Internet befinden. In dieser Abbildung wird ein beliebiger Reverse-Proxy verwendet. Weitere Einzelheiten entnehmen Sie der Dokumentation dieser Anwendung.



Administrationsserver im lokalen Netzwerk; verwaltete Geräte stellen über einen Reverse-Proxy eine Verbindung zum Administrationsserver her

Dieses Verteilungsschema wird empfohlen, wenn Sie nicht möchten, dass die mobilen Geräte sich direkt mit dem Administrationsserver verbinden, und kein Verbindungs-Gateway in der DMZ zuweisen möchten.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, dass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server, oder Port 1433 für Microsoft SQL Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den TLS-Port 13000 zu verwenden.

   > Der Verteilungspunkt wurde in früheren Versionen von Kaspersky Security Center "Update-Agent" genannt.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Die Daten der MMC-basierten Verwaltungskonsole werden über Port 13291 an den Administrationsserver übertragen (Der Administrationsserver kann auf dem gleichen oder einem anderen Gerät installiert sein).

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   9a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Web Console von Kaspersky Security Center kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

10. Nur für mobile Android-Geräte: Daten vom Administrationsserver werden an die Google-Server übermittelt. Über diese Verbindung werden mobile Android-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

11. Nur für mobile Android-Geräte: Push-Benachrichtigungen werden von den Google-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

12. Nur für mobile iOS-Geräte: Daten vom iOS MDM-Server werden an die Apple-Server für Push-Benachrichtigungen übermittelt. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

13. Nur für mobile iOS-Geräte: Push-Benachrichtigungen werden von Apple-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile iOS-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

14. Nur für mobile Geräte: Die Daten des verwalteten Programms werden über den TLS-Port 13292 / 13293 an den Administrationsserver (oder an das Verbindungs-Gateway) übertragen (entweder direkt oder über einen Reverse-Proxy).

15. Nur für mobile Geräte: Daten vom mobilen Gerät werden an die Infrastruktur von Kaspersky übermittelt.

    Wenn das mobile Gerät über keinen Internetzugang verfügt, werden die Daten an den Administrationsserver über den Port 17100 gesendet, und der Administrationsserver sendet diese anschließend an die Kaspersky-Infrastruktur. Allerdings wird dieses Szenario nur selten verwendet.

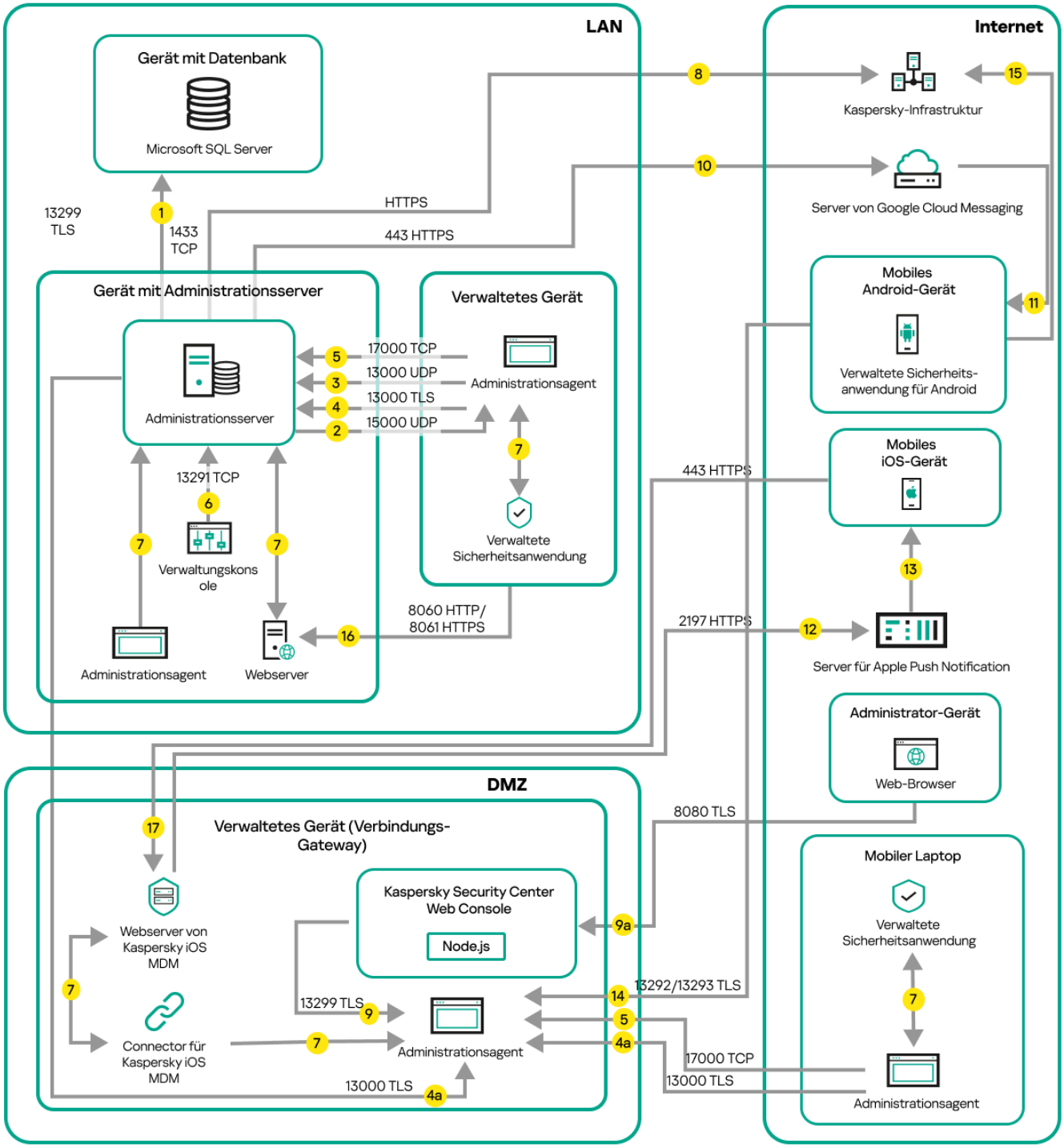
16. Anfragen für Pakete von verwalteten Geräten, einschließlich mobilen Geräten, werden an den Webserver übermittelt, der sich auf demselben Gerät befindet wie der Administrationsserver.

17. Nur für mobile iOS-Geräte: Die Daten von mobilen Geräten werden über den TLS-Port 443 an den iOS MDM-Server übermittelt. Dieser befindet sich auf demselben Gerät wie der Administrationsserver oder auf dem Verbindungs-Gateway.

Administrationsserver im LAN, verwaltete Geräte im Internet; Verwendung eines Verbindungs-Gateways

Die folgende Abbildung zeigt den Datenverkehr für das Szenario, bei dem sich der Administrationsserver im lokalen Netzwerk (LAN) befindet, während sich die verwalteten Geräte – einschließlich mobiler Geräte – im Internet befinden. Ein Verbindungs-Gateway wird verwendet.

Dieses Verteilungsschema wird empfohlen, wenn Sie nicht möchten, dass die mobilen Geräte sich direkt mit dem Administrationsserver verbinden, und weder einen Reverse-Proxy noch eine Unternehmens-Firewall nutzen möchten.



Verwaltete mobile Geräte, die über ein Verbindungs-Gateway mit dem Administrationsserver verbunden sind

In dieser Abbildung sind die verwalteten Geräte über ein Verbindungs-Gateway, welches sich in der DMZ befindet, mit dem Administrationsserver verbunden. Es wird kein Reverse-Proxy und keine Unternehmens-Firewall verwendet.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, d1ass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server, oder Port 1433 für Microsoft SQL Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den TLS-Port 13000 zu verwenden.

   > Der Verteilungspunkt wurde in früheren Versionen von Kaspersky Security Center "Update-Agent" genannt.

   4a. Ein in der DMZ vorhandenes Verbindungs-Gateway empfängt ebenfalls Verbindungen vom Administrationsserver über den TLS-Port 13000. Da ein Verbindungs-Gateway innerhalb der demilitarisierten Zone die Ports des Administrationsservers nicht erreichen kann, etabliert und erhält der Administrationsserver eine permanente Signalverbindung mit einem Verbindungs-Gateway. Die Signalverbindung wird nicht zum Datentransfer verwendet, sondern lediglich, um eine Einladung zur Netzwerk-Interaktion zu übertragen. Wenn ein Verbindungs-Gateway eine Verbindung zum Administrationsserver benötigt, informiert das Gateway den Server mittels der Signalverbindung darüber und anschließend stellt der Server die benötigte Verbindung für den Datentransfer her.

   Mobile Geräte verbinden sich mit dem Verbindungs-Gateway ebenfalls über den TLS-Port 13000.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Die Daten der MMC-basierten Verwaltungskonsole werden über Port 13291 an den Administrationsserver übertragen (Der Administrationsserver kann auf dem gleichen oder einem anderen Gerät installiert sein).

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   9a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Web Console von Kaspersky Security Center kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

10. Nur für mobile Android-Geräte: Daten vom Administrationsserver werden an die Google-Server übermittelt. Über diese Verbindung werden mobile Android-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

11. Nur für mobile Android-Geräte: Push-Benachrichtigungen werden von den Google-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

12. Nur für mobile iOS-Geräte: Daten vom iOS MDM-Server werden an die Apple-Server für Push-Benachrichtigungen übermittelt. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

13. Nur für mobile iOS-Geräte: Push-Benachrichtigungen werden von Apple-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile iOS-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

14. Nur für mobile Geräte: Die Daten des verwalteten Programms werden über den TLS-Port 13292 / 13293 an den Administrationsserver (oder an das Verbindungs-Gateway) übertragen (entweder direkt oder über einen Reverse-Proxy).

15. Nur für mobile Geräte: Daten vom mobilen Gerät werden an die Infrastruktur von Kaspersky übermittelt.

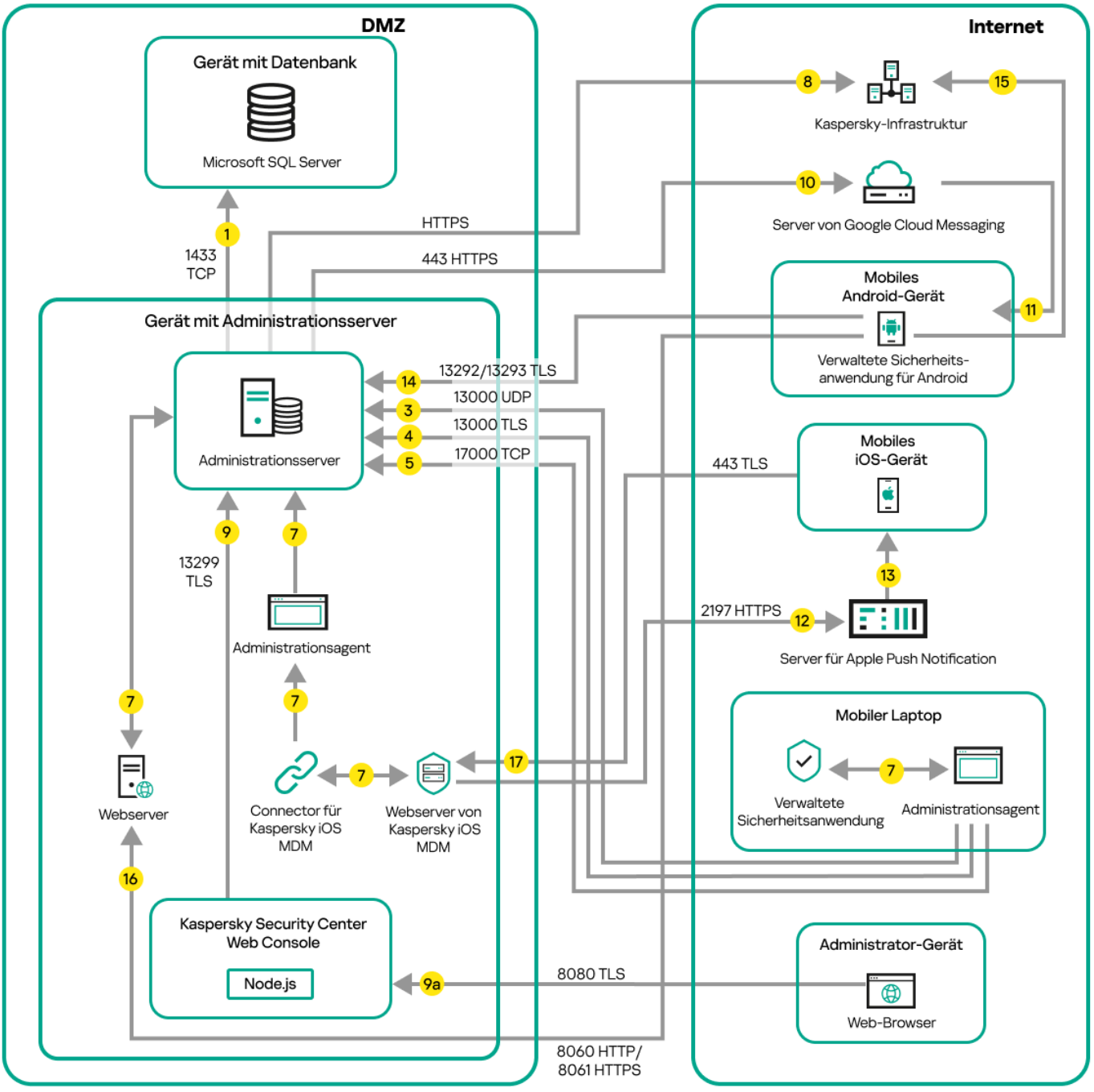
    Wenn das mobile Gerät über keinen Internetzugang verfügt, werden die Daten an den Administrationsserver über den Port 17100 gesendet, und der Administrationsserver sendet diese anschließend an die Kaspersky-Infrastruktur. Allerdings wird dieses Szenario nur selten verwendet.

16. Anfragen für Pakete von verwalteten Geräten, einschließlich mobilen Geräten, werden an den Webserver übermittelt, der sich auf demselben Gerät befindet wie der Administrationsserver.

17. Nur für mobile iOS-Geräte: Die Daten von mobilen Geräten werden über den TLS-Port 443 an den iOS MDM-Server übermittelt. Dieser befindet sich auf demselben Gerät wie der Administrationsserver oder auf dem Verbindungs-Gateway.

Administrationsserver in der DMZ, verwaltete Geräte im Internet

Die folgende Abbildung zeigt den Datenverkehr für das Szenario, bei dem sich der Administrationsserver in der demilitarisierten Zone (DMZ) befindet, während sich die verwalteten Geräte einschließlich mobiler Geräte im Internet befinden.



Administrationsserver in der DMZ, verwaltete mobile Geräte im Internet

In dieser Abbildung wird kein Verbindungs-Gateway verwendet: Die mobilen Geräte stellen eine Direktverbindung zum Administrationsserver her.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, d1ass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server, oder Port 1433 für Microsoft SQL Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den TLS-Port 13000 zu verwenden.

   > Der Verteilungspunkt wurde in früheren Versionen von Kaspersky Security Center "Update-Agent" genannt.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Die Daten der MMC-basierten Verwaltungskonsole werden über Port 13291 an den Administrationsserver übertragen (Der Administrationsserver kann auf dem gleichen oder einem anderen Gerät installiert sein).

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   9a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Web Console von Kaspersky Security Center kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

10. Nur für mobile Android-Geräte: Daten vom Administrationsserver werden an die Google-Server übermittelt. Über diese Verbindung werden mobile Android-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

11. Nur für mobile Android-Geräte: Push-Benachrichtigungen werden von den Google-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

12. Nur für mobile iOS-Geräte: Daten vom iOS MDM-Server werden an die Apple-Server für Push-Benachrichtigungen übermittelt. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

13. Nur für mobile iOS-Geräte: Push-Benachrichtigungen werden von Apple-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile iOS-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

14. Nur für mobile Geräte: Die Daten des verwalteten Programms werden über den TLS-Port 13292 / 13293 an den Administrationsserver (oder an das Verbindungs-Gateway) übertragen (entweder direkt oder über einen Reverse-Proxy).

15. Nur für mobile Geräte: Daten vom mobilen Gerät werden an die Infrastruktur von Kaspersky übermittelt.

    Wenn das mobile Gerät über keinen Internetzugang verfügt, werden die Daten an den Administrationsserver über den Port 17100 gesendet, und der Administrationsserver sendet diese anschließend an die Kaspersky-Infrastruktur. Allerdings wird dieses Szenario nur selten verwendet.

16. Anfragen für Pakete von verwalteten Geräten, einschließlich mobilen Geräten, werden an den Webserver übermittelt, der sich auf demselben Gerät befindet wie der Administrationsserver.

17. Nur für mobile iOS-Geräte: Die Daten von mobilen Geräten werden über den TLS-Port 443 an den iOS MDM-Server übermittelt. Dieser befindet sich auf demselben Gerät wie der Administrationsserver oder auf dem Verbindungs-Gateway.

Interaktion der Komponenten von Kaspersky Security Center und der Sicherheitsanwendungen: weitere Informationen

Dieser Abschnitt enthält die Interaktionsschemata zwischen den Komponenten von Kaspersky Security Center und den verwalteten Sicherheitsanwendungen. In den Schemata sind die Portnummern, die geöffnet sein müssen, sowie die Namen der Prozesse, mit denen die Ports geöffnet werden, angeführt.

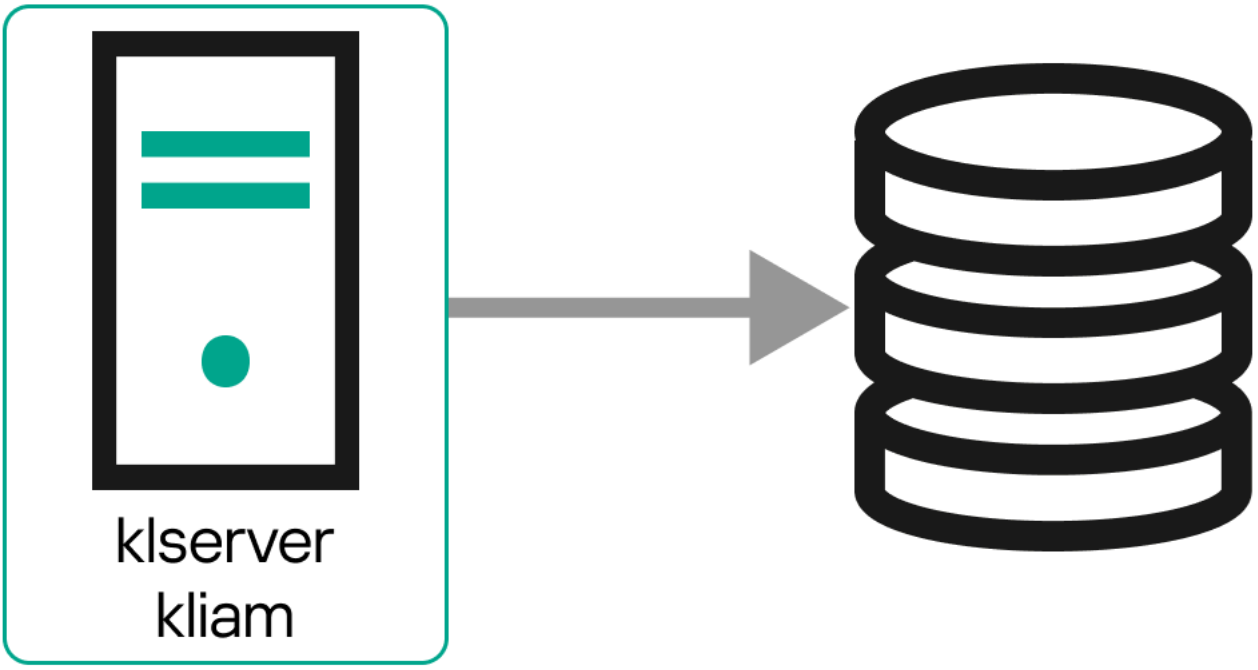
Konventionen für die Interaktionsschemata

In der nachfolgenden Tabelle sind die festgelegten Bezeichnungen angeführt, die in den Schemas verwendet werden.

Zeichen	Erklärung
	Administrationsserver
	Sekundärer Administrationsserver
	DBMS
	Client-Gerät, auf dem der Administrationsagent und ein Programm der Reihe Kaspersky Endpoint Security (oder einer anderen Sicherheitsanwendung, die von Kaspersky Security Center verwaltet werden kann) installiert sind
	Verbindungs-Gateway
	Verteilungspunkt
	Mobiles Client-Gerät mit Kaspersky Security für mobile Endgeräte
	Browser auf dem Gerät des Benutzers
	Prozess, der auf dem Gerät gestartet wird und bestimmte Ports öffnet
	Port und Nummer
	TCP-Datenverkehr (die Pfeilrichtung bezeichnet die Richtung des Verkehrs)
	UDP-Datenverkehr (die Pfeilrichtung bezeichnet die Richtung des Verkehrs)
	COM-Aufruf
	DBMS-Transport
	Grenze der demilitarisierten Zone

Administrationsserver und DBMS

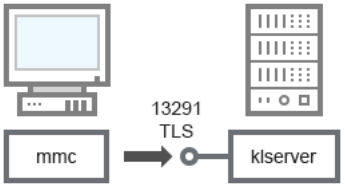
Die Daten werden vom Administrationsserver an die SQL Server-, MySQL- oder MariaDB-Datenbank übermittelt.



Administrationsserver und DBMS

Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server, oder Port 1433 für Microsoft SQL Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

Administrationsserver und Verwaltungskonsole



Administrationsserver und Verwaltungskonsole

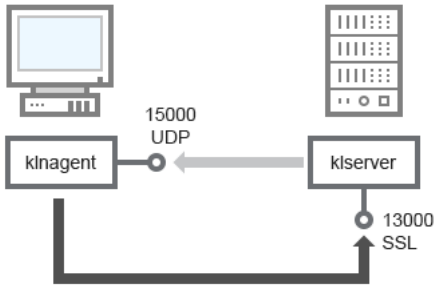
Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver und Verwaltungskonsole (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS	Zweck des Ports
Administrationsserver	13291	klserver	TCP	Ja	Annahme der Verbindungen von der Verwaltungskonsole

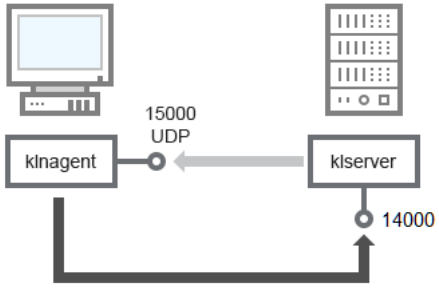
Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendung

Der Administrationsserver nimmt die Verbindungen der Administrationsagenten über den geschützten Port 13000 (SSL) an (s. Abb. unten).



Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendungen, Verbindung über Port 13000 (empfohlen)

Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den ungeschützten Port 14000 (kein SSL) annehmen (s. Abb. unten). Kaspersky Security Center 15.1 unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den SSL-Port 13000 zu verwenden.



Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendungen, Verbindung über Port 14000 (niedrigere Sicherheit)

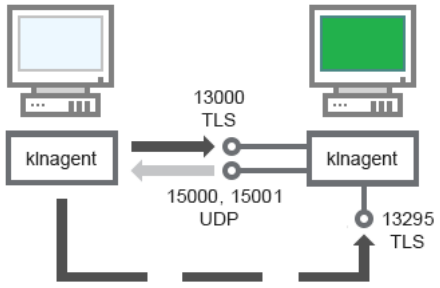
Erklärungen zum Schema finden Sie in den nachfolgenden Tabellen.

Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendung (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS (nur für TCP)	Zweck des Ports
Administrationsagent	15000	klnagent	UDP	Leer	Multicast an die Administrationsagenten
Administrationsserver	13000	klserver	TCP	Ja	Annahme der Verbindungen von den Administrationsagenten
Administrationsserver	14000	klserver	TCP	Nein	Annahme der Verbindungen von den Administrationsagenten

Software-Upgrades auf dem Client-Gerät mithilfe des Verteilungspunkts

Das Client-Gerät stellt eine Verbindung zum Verteilungspunkt über den Port 13000 und, falls Sie den Verteilungspunkt als Push-Server verwenden, über den Port 13295 her; der Verteilungspunkt verwendet Port 15000 für Multicast an die Administrationsagenten (s. Abb. unten). Updates und Installationspakete werden von einem Verteilungspunkt über Port 15001 empfangen.



Software-Update auf dem Client-Gerät über einen Verteilungspunkt

Erklärungen zum Schema finden Sie in der unteren Tabelle.

Software-Update über einen Verteilungspunkt (Datenverkehr)

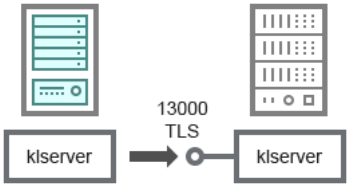
Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS (nur für TCP)	Zweck des Ports
Administrationsagent	15000	klnagent	UDP	Leer	Multicast an die Administrationsagenten
Administrationsagent	15001	klnagent	UDP	Leer	Empfang von Updates und Installationspaketen von einem Verteilungspunkt
Verteilungspunkt	13000	klnagent	TCP	Ja	Annahme der Verbindungen von den Administrationsagenten
Verteilungspunkt	13295	klnagent	TCP	Ja	Verbindungen von Client-Geräten empfangen (mittels Push-Servers)

Hierarchie der Administrationsserver: primärer Administrationsserver und sekundärer Administrationsserver

Das Schema (s. Abb. unten) zeigt, wie der Port 13000 für die Interaktion der Administrationsserver, die in der Hierarchie zusammengefasst sind, verwendet wird.

Bei der Zusammenfassung der Administrationsserver in der Hierarchie ist es erforderlich, dass der Port 13291 beider Server verfügbar ist. Durch den Port 13291 erfolgt die Verbindung der Verwaltungskonsole mit dem Administrationsserver.

Im Weiteren können Sie nach der Zusammenfassung der Server und der Hierarchie beide Server über die Verwaltungskonsole verwalten, die mit dem primären Administrationsserver verbunden ist. Auf diese Weise muss nur der Port 13291 des primären Administrationsservers verfügbar sein.



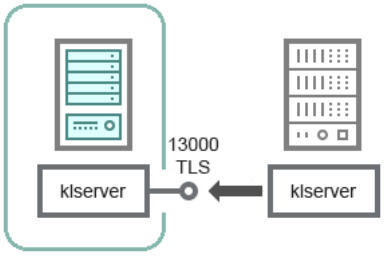
Hierarchie der Administrationsserver: primärer Administrationsserver und sekundärer Administrationsserver

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver-Hierarchie (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS	Zweck des Ports
Primärer Administrationsserver	13000	klserver	TCP	Ja	Empfangen von Verbindungen von sekundären Administrationsservern

Hierarchie der Administrationsserver mit sekundärem Administrationsserver in der demilitarisierten Zone



Hierarchie der Administrationsserver mit sekundärem Administrationsserver in der demilitarisierten Zone

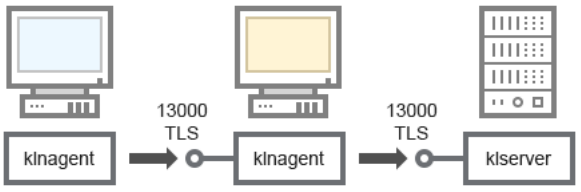
Das Schema zeigt die Hierarchie der Administrationsserver, in welcher der sekundäre Administrationsserver, der sich in der demilitarisierten Zone befindet, die Verbindung vom primären Administrationsserver übernimmt (eine Erklärung zum Schema finden Sie in der nachstehenden Tabelle). Bei der Zusammenfassung der Administrationsserver in der Hierarchie ist es erforderlich, dass der Port 13291 beider Server verfügbar ist. Durch den Port 13291 erfolgt die Verbindung der Verwaltungskonsole mit dem Administrationsserver.

Im Weiteren können Sie nach der Zusammenfassung der Server und der Hierarchie beide Server über die Verwaltungskonsole verwalten, die mit dem primären Administrationsserver verbunden ist. Auf diese Weise muss nur der Port 13291 des primären Administrationsservers verfügbar sein.

Hierarchie der Administrationsserver mit einem sekundären Administrationsserver in der demilitarisierten Zone (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS	Zweck des Ports
Sekundärer Administrationsserver	13000	klserver	TCP	Ja	Aufnahme der Verbindungen vom primären Administrationsserver

Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät



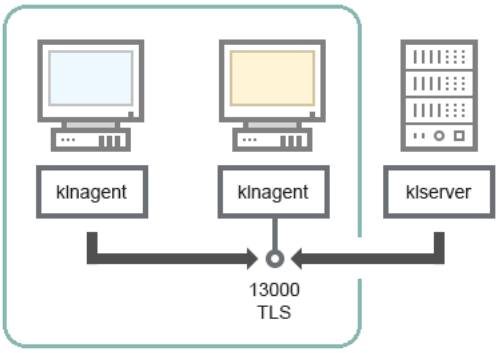
Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS	Zweck des Ports
Administrationsserver	13000	klserver	TCP	Ja	Annahme der Verbindungen von den Administrationsagenten
Administrationsagent	13000	klnagent	TCP	Ja	Annahme der Verbindungen von den Administrationsagenten

Administrationsserver und zwei Geräte in der DMZ: ein Verbindungs-Gateway und ein Client-Gerät



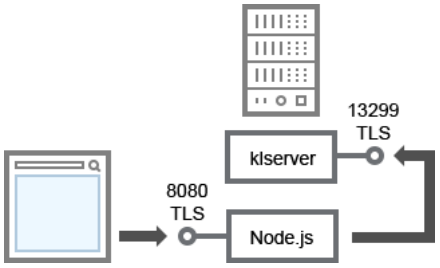
Administrationsserver Verbindungs-Gateway und Client-Gerät in der demilitarisierten Zone

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS	Zweck des Ports
Administrationsagent	13000	klnagent	TCP	Ja	Annahme der Verbindungen von den Administrationsagenten

Administrationsserver und Kaspersky Security Center Web Console



Administrationsserver und Kaspersky Security Center Web Console

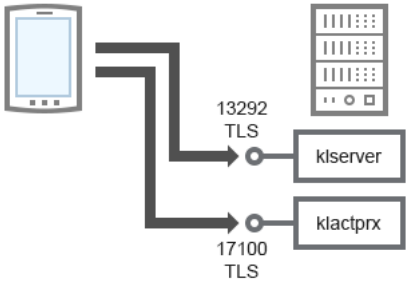
Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver und Kaspersky Security Center Web Console (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS	Zweck des Ports
Administrationsserver	13299	klserver	TCP	Ja	Aufbau von Verbindungen von der Kaspersky Security Center Web Console mit dem Administrationsserver über OpenAPI
Server der Web Console von Kaspersky Security Center oder Administrationsserver	8080	Node.js: Serverseitiges JavaScript	TCP	Ja	Empfangen von Verbindungen von Kaspersky Security Center Web Console

Die Kaspersky Security Center Web Console kann auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

Aktivierung und Verwaltung der Sicherheitsanwendung auf dem mobilen Gerät



Aktivierung und Verwaltung der Sicherheitsanwendung auf dem mobilen Gerät

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Aktivierung und Verwaltung der Sicherheitsanwendung auf dem mobilen Gerät (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	TLS	Zweck des Ports
Administrationsserver	13292	klserver	TCP	Ja	Annahme der Verbindungen von der Verwaltungskonsole zum Administrationsserver
Administrationsserver	17100	klactprx	TCP	Ja	Annahme der Verbindungen zur Anwendungsaktivierung auf mobilen Geräten

Beste Vorgehensweisen für die Bereitstellung

Kaspersky Security Center ist ein verteiltes Programm. Im Lieferumfang von Kaspersky Security Center sind folgende Komponenten enthalten:

- Administrationsserver – die zentrale Komponente, die für die Verwaltung der Geräte des Unternehmens und für die Datenspeicherung im DBMS verantwortlich ist.
- Verwaltungskonsole – das grundlegende Werkzeug des Administrators. Die Verwaltungskonsole wird zusammen mit dem Administrationsserver geliefert, kann aber auch separat auf einem oder mehreren Geräten des Administrators installiert sein.
- Administrationsagent – dient zur Verwaltung der auf dem Gerät installierten Sicherheitsanwendung sowie zum Empfangen von Informationen über das Gerät und zum Übertragen dieser Informationen an den Administrationsserver. Die Administrationsagenten werden auf den Geräten des Unternehmens installiert.

Die Bereitstellung von Kaspersky Security Center im Netzwerk des Unternehmens verläuft auf folgende Weise:

- Installation des Administrationsservers
- Installation der Verwaltungskonsole auf dem Gerät des Administrators
- Installation des Administrationsagenten und der Sicherheitsanwendung auf den Geräten des Unternehmens

Leitfaden zur Härtung

Das Programm Kaspersky Security Center dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentral zu erledigen. Das Programm bietet dem Administrator Zugriff auf detaillierte Informationen über die Qualität der Netzwerksicherheit der Organisation. Mit Kaspersky Security Center können Sie alle Schutzkomponenten konfigurieren, die mithilfe von Kaspersky-Anwendungen erstellt wurden.

Der Kaspersky Security Center Administrationsserver hat vollen Zugriff auf die Schutzverwaltung der Client-Geräte und ist die wichtigste Komponente des Sicherheitssystems der Organisation. Daher sind für den Administrationsserver erhöhte Schutzmaßnahmen erforderlich.

Erstellen Sie vor der Konfiguration eine Backup-Kopie des Kaspersky Security Center Administrationsservers mittels der Aufgabe Backup der Daten des Administrationsservers anlegen oder des Tools "klbackup" und speichern Sie sie an einem sicheren Ort.

Der Leitfaden zur Härtung beschreibt Empfehlungen und Funktionen zur Konfiguration von Kaspersky Security Center und seinen Komponenten, mit dem Ziel, das Risiko einer Kompromittierung zu verringern.

Der Leitfaden zur Härtung enthält die folgenden Informationen:

- Auswahl der Administrationsserver-Architektur
- Konfigurieren einer sicheren Verbindung zum Administrationsserver

- Konfigurieren der Benutzerkonten, um auf den Administrationsserver zuzugreifen
- Verwaltung des Schutzes des Administrationsservers
- Verwaltung des Schutzes der Client-Geräte
- Konfigurieren des Schutzes für verwaltete Programme
- Wartung des Administrationsservers
- Übertragen von Informationen an Drittanbieter-Anwendungen
- Sicherheitsempfehlungen für Drittanbieter-Informationssysteme

Bereitstellung des Administrationsservers

Architektur des Administrationsservers

Im Allgemeinen hängt die Wahl einer zentralisierten Verwaltungsarchitektur von Punkten wie dem Standort der geschützten Geräte, dem Zugriff von benachbarten Netzwerken und den Bereitstellungsschemata für Datenbankaktualisierungen ab.

In der Anfangsphase der Architekturentwurfs empfehlen wir, sich mit den Komponenten von Kaspersky Security Center und ihren Wechselwirkungen untereinander, sowie mit den Schemata für Datenverkehr und Portnutzung vertraut zu machen.

Basierend auf diesen Informationen können Sie eine Architektur entwerfen, die auf Folgendes eingeht:

- Standort des Administrationsservers und Netzwerkverbindungen
- Organisation der Arbeitsbereiche des Administrators und Verbindungsmethoden zum Administrationsserver
- Methoden zur Bereitstellung des Administrationsagenten und der Schutzprogramme
- Verwendung von Verteilungspunkten
- Verwendung von virtuellen Administrationsservern
- Verwendung einer Administrationsserver-Hierarchie
- Update-Schema für Antiviren-Datenbanken
- Weitere Datenflüsse

Auswahl eines Geräts zur Installation des Administrationsservers

Wir empfehlen, dass Sie den Administrationsserver auf einem dedizierten Server in der Infrastruktur Ihrer Organisation installieren. Wenn auf dem Server keine weiteren Drittanbieter-Programme installiert sind, können Sie die Sicherheitseinstellungen gemäß den Anforderungen von Kaspersky Security Center konfigurieren, ohne von den Anforderungen der Drittanbieter-Programme abhängig zu sein.

Sie können den Administrationsserver auf einem physischen Server oder auf einem virtuellen Server bereitstellen. Stellen Sie sicher, dass das ausgewählte Gerät die Hardware- und Softwareanforderungen erfüllt.

Standort des Administrationsservers

Vom Administrationsserver verwaltete Geräte können in folgenden Standorten platziert werden:

- In einem lokalen Netzwerk (LAN)
- Im Internet
- In der entmilitarisierten Zone (DMZ)

Gleichzeitig kann sich der Administrationsserver auch in verschiedenen Segmenten befinden, etwa Industrie-, Unternehmens- und DMZ-Segmente.

Wenn Sie Kaspersky Security Center dazu verwenden, den Schutz eines isolierten Netzwerksegments zu verwalten, empfehlen wir die Bereitstellung des Administrationsservers in einem Segment der demilitarisierten Zone (DMZ). Auf diese Weise können Sie eine ordnungsgemäße Netzwerksegmentierung organisieren und den Datenverkehr zum geschützten Segment minimieren, während die vollständigen Verwaltungsfunktionen und die Verteilung von Updates erhalten bleiben.

Einschränkung bei der Bereitstellung des Administrationsservers auf einem Domänencontroller, Terminalserver oder Benutzergerät

Wir raten dringend davon ab, den Administrationsserver auf einem Domänencontroller, Terminalserver oder Benutzergerät zu installieren.

Wir empfehlen, dass Sie für die Schlüsselknoten des Netzwerks eine funktionale Trennung vorzusehen. Mit diesem Ansatz können Sie die Funktionsfähigkeit verschiedener Systeme aufrechterhalten, wenn ein Knoten ausfällt oder kompromittiert wird. Gleichzeitig können Sie für jeden Knoten unterschiedliche Sicherheitsrichtlinien erstellen.

Beispielsweise können Sicherheitsbeschränkungen, die normalerweise auf einen Domänencontroller angewendet werden, die Leistung des Administrationsservers erheblich beeinträchtigen und die Nutzung einiger Funktionen des Administrationsservers unmöglich machen. Wenn ein Eindringling privilegierten Zugriff auf den Domänencontroller erlangt, kann die Datenbank des Active Directory Domain Service (AD DS) verändert, beschädigt oder zerstört werden. Darüber hinaus können alle von Active Directory verwalteten Systeme und Konten kompromittiert werden.

Konten für die Installation und Ausführung des Administrationsservers

Wir empfehlen, die Installation des Administrationsservers unter einem lokalen Administratorkonto auszuführen, um die Verwendung von Domänenkonten für den Zugriff auf die Administrationsserver-Datenbank zu vermeiden. Die Art und der Umfang der erforderlichen Benutzerkonten und deren Rechte hängen vom ausgewählten DBMS-Typ, dem DBMS-Speicherort und der Methode zur Erstellung der Administrationsserver-Datenbank ab.

Bei der Installation von Kaspersky Security Center werden die Gruppen "KLAdmins" und "KLOperators" automatisch erstellt. Diesen Gruppen werden die Rechte für die Verbindung mit dem Administrationsserver und die Bearbeitung der Serverobjekte gewährt.

Abhängig davon, unter welchem Benutzerkonto Kaspersky Security Center installiert wird, werden die Gruppen "KLAdmins" und "KLOperators" auf folgende Weise erstellt:

- Wenn die Installation unter einem Benutzerkonto ausgeführt wird, das zu einer Domäne gehört, werden die Gruppen auf dem Gerät des Administrationsservers sowie in der Domäne, zu welcher der Administrationsserver gehört, erstellt.

- Wenn die Installation unter einem System-Benutzerkonto ausgeführt wird, werden die Gruppen nur auf dem Gerät des Administrationsserver erstellt.

Um zu vermeiden, dass in der Domäne die Gruppen "KLAdmins" und "KLOperators" erstellt werden und dadurch **Berechtigungen zur Verwaltung des Administrationsservers einem Konto außerhalb des Geräts mit dem Administrationsserver erteilt werden** können, empfehlen wir, Kaspersky Security Center unter einem lokalen Konto zu installieren.

Wählen während der Installation des Administrationsservers ein Benutzerkonto aus, unter dem der Administrationsserver als Dienst gestartet werden soll. Standardmäßig erstellt das Programm ein lokales Konto namens "KL-AK-*", unter dem der Dienst des Administrationsservers (Dienst "klserver") ausgeführt wird.

Bei Bedarf kann der Dienst des Administrationsservers unter dem ausgewählten Konto ausgeführt werden. Diesem Konto müssen die erforderlichen Rechte für den Zugriff auf das DBMS gewährt werden. Verwenden Sie aus Sicherheitsgründen ein nicht-privilegiertes Konto für die Ausführung des Administrationsserver-Dienstes.

Um die Verwendung einer falscher Kontokonfiguration zu vermeiden, empfehlen wir, das Konto automatisch zu erstellen.

Ausschluss des Administrationsservers aus einer Domäne

Wenn Sie den Administrationsserver verwenden, um Gerätegruppen mit kritischen Systemen zu schützen, wird es davon abgeraten, das Gerät mit dem Administrationsserver in die Domäne aufzunehmen. Auf diese Weise können Sie die Verwaltungsrechte von Kaspersky Security Center differenzieren und den Zugriff auf den Administrationsserver verhindern, falls das Domänenkonto kompromittiert wird.

Beachten Sie, dass die folgenden Szenarien für die Arbeit mit dem Administrationsserver nicht verfügbar sind, wenn Sie den Administrationsserver auf einem Gerät installieren, das zur Arbeitsgruppe gehört:

- Verwendung eines Kaspersky Security Center Failover-Clusters

- Verwendung eines Windows Server Failover-Clusters

- Verwendung von SQL Server für Windows auf einem separaten Gerät

  Sie können SQL Server für Windows nur dann auf einem separaten Gerät verwenden, wenn der Administrationsserver und SQL Server zur gleichen Domäne oder zu vertrauenswürdigen Domänen gehören. Wenn sich der Administrationsserver, SQL Server und eine UNC-Freigabe für Speicher in einer Arbeitsgruppe befinden, können die Zugriffs- und Lese-/Schreibrechte für SQL Server und die Freigabe nicht sicher eingerichtet werden.

- Remote-Installation mittels Tools des Administrationsservers über die Gruppenrichtlinien des Active Directory

Wenn Sie den Administrationsserver von der Active Directory-Domäne trennen müssen, folgen Sie den Schritten, die im Thema So ändern Sie den Namen von Kaspersky Security Center beschrieben werden.

Wenn der Administrationsserver auf einem Gerät der Arbeitsgruppe installiert werden muss, können Sie anstelle von Kaspersky Security Center Windows auch Kaspersky Security Center Linux verwenden.

Verbindungssicherheit

Verwendung von TLS

Wir empfehlen, unsichere Verbindungen zum Administrationsserver zu verbieten. Beispielsweise können Sie in den Einstellungen des Administrationsservers Verbindungen verbieten, die HTTP verwenden.

Beachten Sie, dass standardmäßig einige HTTP-Ports des Administrationsservers geschlossen sind. Der verbleibende Port wird für den Webserver des Administrationsservers (8060) verwendet. Dieser Port kann durch die Firewall-Einstellungen des Administrationsservers eingeschränkt werden.

Restriktive TLS-Einstellungen

Wir empfehlen, das TLS-Protokoll ab Version 1.2 zu verwenden und unsichere Verschlüsselungsalgorithmen einzuschränken oder zu verbieten.

Sie können die vom Administrationsserver verwendeten Verschlüsselungsprotokolle konfigurieren (TLS). Beachten Sie, dass zum Veröffentlichungszeitpunkt einer Administrationsserver-Version die Einstellungen des Verschlüsselungsprotokolls standardmäßig so konfiguriert sind, dass sie eine sichere Datenübertragung gewährleisten.

Verbot der Remote-Authentifizierung durch Verwendung von Windows-Konten

Sie können den Parameter "LP_RestrictRemoteOsAuth"-verwenden, um SSPI-Verbindungen von Remote-Adressen zu verbieten. Mit diesem Parameter können Sie die Remote-Authentifizierung auf dem Administrationsserver unter Verwendung lokaler Konten oder Windows-Domänenkonten verbieten.

So setzen Sie den Parameter "LP_RestrictRemoteOsAuth-Flag" für den Modus zum Verbieten von Verbindungen mit Remote-Adressen:

1. Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet <Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center.

2. Führen Sie den folgenden Befehl in der Befehlszeile aus, um den Wert des Flags "LP_RestrictRemoteOsAuth" anzugeben:

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. Starten Sie den Dienst des Administrationsservers neu.

Der Parameter "LP_RestrictRemoteOsAuth" funktioniert nicht, wenn die Remote-Authentifizierung über die Kaspersky Security Center Web Console oder die Verwaltungskonsole durchgeführt wird, die auf dem Gerät mit dem Administrationsserver installiert ist.

Einschränkung des Zugriffs auf die Administrationsserver-Datenbank

Wir empfehlen eine Einschränkung des Zugriffs auf die Administrationsserver-Datenbank. Beispielsweise können Sie den Zugriff lediglich vom Gerät des Administrationsservers aus zulassen. Dadurch wird die Wahrscheinlichkeit verringert, dass die Administrationsserver-Datenbank aufgrund bekannter Schwachstellen kompromittiert wird.

Sie können die Parameter gemäß dem Handbuch der verwendeten Datenbank konfigurieren sowie geschlossene Ports auf Firewalls bereitstellen.

Authentifizierung von Microsoft SQL Server

Wenn Kaspersky Security Center als DBMS Microsoft SQL Server verwendet, ist es notwendig, von Kaspersky Security Center benötigte Daten, die in die oder aus der Datenbank übertragen werden, sowie Daten, die in der Datenbank gespeichert werden, vor unbefugtem Zugriff zu schützen. Dazu müssen Sie eine sichere Kommunikation zwischen Kaspersky Security Center und SQL Server gewährleisten. Die zuverlässigste Möglichkeit zur Bereitstellung einer sicheren Kommunikation besteht darin, Kaspersky Security Center und SQL Server auf demselben Gerät zu installieren und den Mechanismus für gemeinsame Speichernutzung für beide Anwendungen zu verwenden. In allen anderen Fällen empfehlen wir die Verwendung eines SSL-/TLS-Zertifikats zur Authentifizierung der SQL Server-Instanz.

Im Allgemeinen kann der Administrationsserver einen SQL Server über die folgenden Provider adressieren:

- SQLOLEDB mittels TCP/IP oder Named Pipes

  Dieser ist Teil des Windows-Betriebssystems und wird standardmäßig verwendet.

- MSOLEDBSQL mittels TCP/IP, Named Pipes oder Shared-Speicher

  Wenn Sie diesen Provider verwenden möchten, müssen Sie ihn auf dem Gerät mit dem Administrationsserver installieren und anschließend den Wert der globalen Umgebungsvariable `KLDBADO_UseMSOLEDBSQL` auf `1` setzen.

- MSOLEDBSQL19 mittels TCP/IP, Named Pipes oder Shared-Speicher

  Wenn Sie diesen Provider verwenden möchten, müssen Sie ihn auf dem Gerät mit dem Administrationsserver installieren und anschließend den Wert der globalen Umgebungsvariable `KLDBADO_UseMSOLEDBSQL` auf `1` und den Wert der globalen Umgebungsvariable `KLDBADO_ProviderName` auf `MSOLEDBSQL19` setzen.

Stellen Sie vor der Verwendung von TCP/IP, Named Pipes oder Shared-Speicher außerdem sicher, dass das erforderliche Protokoll aktiviert ist.

Sichere Interaktion mit einem externen DBMS

Wenn das DBMS während der Installation des Administrationsservers auf einem separaten Gerät installiert wird (externes DBMS), wird es empfohlen, die Parameter für die sichere Interaktion und Authentifizierung mit diesem DBMS anzupassen. Weitere Informationen über die Konfiguration der SSL-Authentifizierung finden Sie im Szenario: Authentifizierung am PostgreSQL-Server und im Szenario: Authentifizierung am MySQL-Server.

Eine Allow-Liste von IP-Adressen für die Verbindung mit dem Administrationsserver konfigurieren

Die Anmeldung an Kaspersky Security Center ist für die Benutzer von Kaspersky Security Center standardmäßig von jedem Gerät aus möglich, auf dem die MMC-basierte Verwaltungskonsole, die Kaspersky Security Center Web Console oder OpenAPI-Anwendungen installiert sind. Sie können den Administrationsserver auch so konfigurieren, dass Benutzer nur von Geräten mit zugelassenen IP-Adressen eine Verbindung zu ihm herstellen dürfen. Wenn beispielsweise eine angreifende Person versucht, sich bei Kaspersky Security Center mittels eines Servers der Kaspersky Security Center Web Console anzumelden, der auf einem Gerät installiert ist, das nicht auf der Allow-Liste steht, kann sich diese Person nicht an Kaspersky Security Center anmelden.

Allow-Liste mit IP-Adressen für die Verbindung mit Kaspersky Security Center Web Console konfigurieren

Standardmäßig können sich Benutzer von Kaspersky Security Center von jedem Gerät aus mit der Kaspersky Security Center Web Console verbinden. Auf einem Gerät mit installierter Kaspersky Security Center Web Console müssen Sie eine Firewall konfigurieren (via Betriebssystem oder Drittanbieter-Anwendung), damit sich Benutzer nur mit erlaubten IP-Adressen mit der Kaspersky Security Center Web Console verbinden können.

Sicherheit der Verbindung mit dem Domänencontroller während der Abfrage

Um die Domäne abzufragen, verbinden sich der Administrationsserver oder ein Linux-Verteilungspunkt per LDAPS mit dem Domänencontroller. Standardmäßig ist bei der Verbindung keine Überprüfung des Zertifikats notwendig. Um die Überprüfung des Zertifikats zu erzwingen, setzen Sie das Flag `KLNAG_LDAP_TLS_REQCERT` auf "1". Sie können außerdem einen benutzerdefinierten Pfad zur Zertifizierungsstelle (CA) angeben, um über das Flag `KLNAG_LDAP_SSL_CACERT` auf die Zertifikatkette zuzugreifen.

Konten und Authentifizierung

Bevor Sie die folgenden Schritte ausführen, erstellen Sie eine Backup-Kopie des Kaspersky Security Center Administrationsservers mithilfe der Aufgabe Backup der Daten des Administrationsservers anlegen oder des Tools "klbackup" und speichern Sie diese an einem sicheren Ort.

Verwendung der zweistufigen Überprüfung mit dem Administrationsserver

Kaspersky Security Center bietet eine zweistufige Überprüfung für Benutzer der Kaspersky Security Center Web Console und der Verwaltungskonsole. Diese basiert auf dem RFC 6238-Standard (TOTP: Time-Based One-Time Password Algorithm).

Wenn die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktiviert ist, müssen Sie bei jeder Anmeldung an der Kaspersky Security Center Web Console oder Verwaltungskonsole den Benutzernamen, das Kennwort und einen zusätzlichen Einmal-Sicherheitscode eingegeben. Wenn Sie für Ihr Konto die Domänenauthentifizierung verwenden, müssen Sie nur einen zusätzlichen Einmal-Sicherheitscode eingeben. Um einen Einmal-Sicherheitscode zu erhalten, müssen Sie eine Authenticator-App auf Ihrem Computer oder mobilen Gerät installieren.

Für den RFC 6238-Standard existieren sowohl Software- als auch Hardware-Authenticators (Token). Zu den Software-Authenticators gehören beispielsweise Google Authenticator, Microsoft Authenticator und FreeOTP.

Wir raten dringend davon ab, die Authenticator-App auf demselben Gerät zu installieren, von dem aus die Verbindung zum Administrationsserver hergestellt wird. Sie können eine Authenticator-App auf Ihrem Mobilgerät installieren.

Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst einschränken

Um die Zugriffssicherheit von Kaspersky Security Center Web Console weiter zu verbessern, können Sie verhindern, dass neue Benutzer die zweistufige Überprüfung für sich selbst einrichten.

Bei aktivierter Option kann ein Benutzer, für den die zweistufige Überprüfung deaktiviert ist (z. B. ein neuer Domänenadministrator) die zweistufige Überprüfung nicht für sich selbst konfigurieren. Auf diese Weise kann ein solcher Benutzer ohne Zustimmung eines weiteren Administrators von Kaspersky Security Center, für den die Zwei-Faktor-Authentifikation bereits aktiviert wurde, nicht am Administrationsserver authentifiziert werden und sich nicht an der Kaspersky Security Center Web Console anmelden.

Verwendung der Zwei-Faktor-Authentifizierung für ein Betriebssystem

Für die Authentifizierung auf dem Gerät des Administrationsservers empfehlen wir die Verwendung der Multi-Faktor-Authentifizierung (MFA) mithilfe eines Tokens, einer Smartcard oder einer anderen Methode (falls möglich).

Speichern des Administratorkennworts einschränken

Wenn Sie die Verwaltungskonsole verwenden, raten wir davon ab, das Administratorkennwort im Feld des Verbindungsdialogs für den Administrationsservers zu speichern.

Wenn Sie Kaspersky Security Center Web Console verwenden, raten wir davon ab, das Administratorkennwort in einem auf dem Benutzergerät installierten Browser zu speichern.

Authentifizierung eines internen Benutzerkontos

Standardmäßig muss das Kennwort eines internen Benutzerkontos des Administrationsservers die folgenden Regeln einhalten:

- Das Kennwort muss zwischen 8 und 256 Zeichen lang sein
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Ziffern (0–9)
  - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

Standardmäßig liegt die maximale Anzahl zulässiger Versuche zur Eingabe eines Kennworts bei 10. Sie können die Anzahl der zulässigen Eingabeversuche für das Kennwort ändern.

Benutzer von Kaspersky Security Center können eine begrenzte Anzahl von ungültigen Kennwörtern eingeben. Wenn das Limit erreicht ist, wird das Benutzerkonto für eine Stunde gesperrt.

Optionen zur Kennwortänderung eines internen Benutzerkontos konfigurieren

Es wird empfohlen, die folgenden Optionen für die Kennwortänderung eines internen Benutzerkontos zu konfigurieren:

- Zeitraum der Kennwortrotation
- Zeitspanne der vorherigen Warnung über eine erforderliche Kennwortänderung
- Wert der Option **Der Benutzer muss bei der ersten Anmeldung das Kennwort ändern**

Schutz von Benutzerkonten vor unbefugten Änderungen

Es wird empfohlen, eine zusätzliche Option zu aktivieren, um interne Benutzerkonten des Administrationsservers unbefugter Änderung zu schützen. Dieser Schutz muss für jeden internen Benutzer separat konfiguriert werden.

Dedizierte Administrationsgruppe für den Administrationsserver

Wir empfehlen die Erstellung einer dedizierten Administrationsgruppe für den Administrationsserver. Gewähren Sie dieser Gruppe gesonderte Zugriffsrechte und erstellen Sie eine gesonderte Sicherheitsrichtlinie für sie.

Um die Sicherheitsstufe des Administrationsservers nicht absichtlich herabzusetzen, empfehlen wir, die Liste der Konten einzuschränken, welche die dedizierte Administrationsgruppe verwalten dürfen.

Die Gruppen "KLAdmins" und "KLOperators"

Bei der Installation von Kaspersky Security Center werden die Gruppen "KLAdmins" und "KLOperators" automatisch erstellt. Der Gruppe "KLAdmins" werden alle Zugriffsrechte gewährt. Der Gruppe "KLOperators" werden nur Lese- und Ausführungsrechte gewährt. Die der Gruppe "KLAdmins" gewährten Berechtigungen sind **gesperrt**.

Sie können die Gruppen "KLAdmins" und "KLOperators" anzeigen und Änderungen an diesen Gruppen vornehmen, indem Sie die standardmäßigen Verwaltungstools des Betriebssystems verwenden.

Bei der Entwicklung von Vorschriften für die Arbeit mit dem Administrationsserver muss festgelegt werden, ob der Spezialist für Informationssicherheit zur Ausführung seiner Aufgaben den vollen Zugriff (und die Aufnahme in die Gruppe "KLAdmins") benötigt.

Die meisten grundlegenden Verwaltungsaufgaben können zwischen Unternehmensabteilungen (oder verschiedenen Mitarbeitern derselben Abteilung) und folglich zwischen verschiedenen Konten verteilt werden. Sie können im Kaspersky Security Center auch eine Differenzierung des Zugriffs für Administrationsgruppen einrichten. Daher ist es möglich, ein Szenario so zu implementieren, dass eine Autorisierung mittels Konten aus der Gruppe "KLAdmins" anomal ist und als Vorfall betrachtet werden könnte.

Wenn Kaspersky Security Center unter einem Systemkonto installiert wurde, werden Gruppen nur auf dem Gerät des Administrationsservers erstellt. In diesem Fall empfehlen wir sicherzustellen, dass nur Einträge in die Gruppe aufgenommen werden, die während der Installation von Kaspersky Security Center erstellt wurden. Wir empfehlen, keine Gruppen zur Gruppe "KLAdmins" (lokal und/oder Domäne) hinzuzufügen, die automatisch während der Installation von Kaspersky Security Center erstellt wird. Sie sollten auch die Rechte zum Ändern dieser Gruppe einschränken. Die Gruppe "KLAdmins" darf nur einzelne nicht-privilegierte Benutzerkonten enthalten.

Wenn die Installation unter einem Domänenbenutzerkonto durchgeführt wurde, werden die Gruppen "KLAdmins" und "KLOperators" sowohl auf dem Administrationsserver als auch in der Domäne erstellt, die den Administrationsserver enthält. Es wird ein ähnlicher Ansatz wie die Installation eines lokalen Kontos wird empfohlen.

Einschränken der Rolle "Hauptadministrator"

Wir empfehlen, für die Rolle "Hauptadministrator" die Zugehörigkeiten einzuschränken.

Standardmäßig wird nach der Installation des Administrationsservers die Rolle "Hauptadministrator" der Gruppe der lokalen Administratoren und der erstellten Gruppe "KLAdmins" zugewiesen. Sie ist für sinnvoll für zur Verwaltung, aber kritisch für die Sicherheit, da die Rolle des Hauptadministrators über umfangreiche Rechte verfügt. Die Vergabe dieser Rolle an Benutzer sollte restriktiv geregelt werden.

Lokale Administratoren können aus der Liste der Benutzer mit Administratorrechten von Kaspersky Security Center ausgeschlossen werden. Die Rolle "Hauptadministrator" kann nicht aus der Gruppe "KLAdmins" entfernt werden. Sie können der Gruppe "KLAdmins" die Konten hinzufügen die zur Verwaltung des Administrationsservers verwendet werden.

Wenn Sie die Domänenauthentifizierung verwenden, empfehlen wir, die Berechtigungen der Administratorkonten der Domäne in Kaspersky Security Center einzuschränken. Standardmäßig besitzen diese Konten die Rolle "Hauptadministrator". Außerdem kann ein Administrator der Domäne sein Konto in die Gruppe "KLAdmins" aufnehmen, um die Rolle "Hauptadministrator" zu erhalten. Um dies zu vermeiden, können Sie in den Sicherheitseinstellungen von Kaspersky Security Center die Gruppe "Domain Admins" hinzufügen und dann Verbotsregeln dafür definieren. Diese Regeln müssen Vorrang vor den Erlaubnisregeln haben.

Sie können auch die vordefinierten Benutzerrollen mit einem bereits konfigurierten Satz von Rechten verwenden.

Zugriffsrechte auf Programmfunktionen konfigurieren

Wir empfehlen, für jeden Benutzer oder jede Benutzergruppe eine flexible Konfiguration der Zugriffsrechte auf die Funktionen von Kaspersky Security Center.

Rollenbasierte Zugriffskontrolle erlaubt das Erstellen typischer Benutzerrollen mit einer vordefinierten Auswahl von Berechtigungen und das Zuweisen dieser Rollen an die Benutzer entsprechend ihrer dienstlichen Verpflichtungen.

Die Hauptvorteile des Modells der rollenbasierten Zugriffskontrolle:

- Einfache Verwaltung
- Rollenhierarchie
- Prinzip der niedrigsten Priorität (POLP)
- Trennung von Aufgaben

Sie können bestimmten Mitarbeitern basierend auf deren Positionen vordefinierte Rollen zuweisen oder neue Rollen erstellen.

Achten Sie bei der Rollenkonfiguration auf die Berechtigungen, die mit der Änderung des Schutzstatus des Geräts mit dem Administrationsserver und der Remote-Installation von Drittanbieter-Programmen verbunden sind:

- Administrationsgruppen verwalten.
- Vorgänge mit dem Administrationsserver.
- Remote-Installation.
- Ändern der Parameter zum Speichern von Ereignissen und Senden von Benachrichtigungen.

  Mit diesem Recht können Sie Benachrichtigungen einrichten, die bei Eintritt eines Ereignisses ein Skript oder ein ausführbares Modul auf dem Gerät des Administrationsservers ausführen.

Separate Benutzerkonten für die Remote-Installation von Programmen

Neben der grundsätzlichen Unterscheidung der Zugriffsrechte empfehlen wir, die Remote-Installation von Programmen für alle Konten einzuschränken (außer für den Hauptadministrator oder ein anderes spezialisiertes Konto).

Für die Remote-Installation von Anwendungen empfehlen die Verwendung eines separaten Benutzerkontos. Sie können dem separaten Benutzerkonto eine Rolle zuweisen oder Berechtigungen zuweisen.

Schützen des privilegierten Zugriffs von Windows

Wir empfehlen, die von Microsoft zur Bereitstellung von privilegierter Zugriffssicherheit veröffentlichten Empfehlungen zu berücksichtigen. Diese Empfehlungen finden Sie im Artikel Schützen des priviligierten Zugriffs.

Einer der wichtigsten Punkte der Empfehlungen ist die Implementierung von Privileged Access Workstations (PAW).

Verwendung eines verwalteten Dienstkontos (Managed Service Account, MSA) oder eines verwalteten Gruppendienstkontos (Group Managed Service Account, gMSA) zum Ausführen des Dienstes des Administrationsservers

Active Directory verfügt über eine spezielle Art von Konten zum sicheren Ausführen von Diensten, genannt Gruppenverwaltetes Dienstkonto (MSA/gMSA). Kaspersky Security Center unterstützt verwaltete Dienstkonten (Managed Service Accounts, MSA) und gruppenverwaltete Dienstkonten (Group Managed Service Accounts, gMSA). Wenn solche Benutzerkonten in Ihrer Domäne verwendet werden, können Sie eines der Konten als Benutzerkonto für den Dienst des Administrationsservers wählen.

Regelmäßiges Audit aller Benutzer und Benutzervorgänge

Wir empfehlen, auf dem Gerät des Administrationsservers eine regelmäßige Überprüfung aller Benutzer durchzuführen. Auf diese Weise können Sie auf bestimmte Arten von Sicherheitsbedrohungen reagieren, die mit einer möglichen Kompromittierung des Geräts verbunden sind.

Außerdem können Sie verschiedene Benutzervorgänge verfolgen, wie etwa: hergestellte und getrennte Verbindungen zum Administrationsserver, fehlerhafte Verbindungen zum Administrationsserver und Objektänderungen (für Objekte, welche die Revisionsverwaltung unterstützen).

Verwaltung des Schutzes des Administrationsservers

Auswahl eines Schutzprogramms für den Administrationsserver

Wählen Sie je nach Einsatzart des Administrationsservers und der allgemeinen Schutzstrategie die Anwendung aus, die das Gerät des Administrationsservers schützen soll.

Wenn Sie den Administrationsserver auf einem dezidierten Gerät bereitstellen, empfehlen wir, Kaspersky Endpoint Security als Anwendung für den Schutz des Geräts mit dem Administrationsserver auszuwählen. Dies ermöglicht die Verwendung aller verfügbaren Technologien zum Schutz des Geräts des Administrationsservers, einschließlich den Modulen zur Verhaltensanalyse.

Wenn der Administrationsserver auf einem Gerät installiert wird, das in der Infrastruktur vorhanden ist und zuvor für andere Aufgaben verwendet wurde, empfehlen wir, die folgende Schutzanwendungen in Betracht zu ziehen:

- Kaspersky Industrial CyberSecurity for Nodes. Wir empfehlen, diese Anwendung auf Geräten zu installieren, die in ein industrielles Netzwerk eingebunden sind. Kaspersky Industrial CyberSecurity for Nodes ist eine Anwendung, die über Kompatibilitätszertifikate mit verschiedenen Herstellern von Industriesoftware verfügt.

- Empfohlene Sicherheitslösungen. Wenn der Administrationsserver auf einem Gerät mit anderer Software installiert ist, empfehlen wir, die Vorgaben dieses Softwareanbieters zur Kompatibilität von Sicherheitslösungen zu berücksichtigen (möglicherweise gibt es bereits Vorgaben zur Auswahl einer Sicherheitslösung, und Sie müssen möglicherweise die vertrauenswürdige Zone konfigurieren).

Erstellen einer separaten Sicherheitsrichtlinie für die Schutzanwendung

Wir empfehlen, dass Sie eine separate Sicherheitsrichtlinie für die Anwendung erstellen, die das Gerät mit dem Administrationsserver schützt. Diese Richtlinie muss sich von der Sicherheitsrichtlinie für Client-Geräte unterscheiden. Dadurch können die am besten geeigneten Sicherheitseinstellungen für den Administrationsserver festgelegt werden, ohne die Schutzstufe anderer Geräte zu beeinträchtigen.

Wir empfehlen, die Geräte in Gruppen zu unterteilen und anschließend das Gerät des Administrationsservers in einer separaten Gruppe zu platzieren, für die Sie eine spezielle Sicherheitsrichtlinie erstellen können.

Schutzmodule

Wenn es für die Drittanbieter-Programme, die auf dem Gerät mit dem Administrationsserver installiert sind, keine besonderen Empfehlungen vom Hersteller der gibt, empfehlen wir, alle verfügbaren Schutzmodule zu aktivieren und zu konfigurieren. Dem sollte ausreichend Zeit zur Überprüfung der Ausführung dieser Schutzmodule vorausgehen.

Konfiguration der Firewall des Administrationsserver-Geräts

Auf dem Gerät mit dem Administrationsserver empfehlen wir die Firewall so zu konfigurieren, dass die Anzahl derjenigen Geräte, von denen Administratoren über die Verwaltungskonsole oder die Kaspersky Security Center Web Console eine Verbindung zum Administrationsserver herstellen können, eingeschränkt wird.

Standardmäßig verwendet der Administrationsserver den Port 13291 zum Empfangen von Verbindungen von der Verwaltungskonsole und Port 13299 zum Empfangen von Verbindungen von der Kaspersky Security Center Web Console. Wir empfehlen, die Anzahl der Geräte zu beschränken, von denen der Administrationsserver über diese Ports verwaltet werden kann.

Verwaltung des Schutzes der Client-Geräte

Einschränken des Hinzufügens von Lizenzschlüsseln zu Installationspaketen

Installationspakete werden im freigegebenen Ordner des Administrationsservers im Unterordner "Pakete" gespeichert. Wenn Sie einem Installationspaket einen Lizenzschlüssel hinzufügen, kann der Lizenzschlüssel kompromittiert werden, da für die Datenverwaltung mit den Installationspaketen gemeinsame Leseberechtigungen aktiviert sind.

Um eine Gefährdung des Lizenzschlüssels zu vermeiden, raten wir davon ab, Lizenzschlüssel zu den Installationspaketen hinzuzufügen.

Wir empfehlen für die Bereitstellung die Verwendung der automatischen Verteilung von Lizenzschlüsseln an verwaltete Geräte mithilfe der Aufgabe "Hinzufügen eines Lizenzschlüssels für ein verwaltetes Programm" und manuelles Hinzufügen eines Aktivierungscodes oder einer Schlüsseldatei zu den Geräten.

Automatische Regeln für das Verschieben von Geräten zwischen Administrationsgruppen

Wir empfehlen, die Verwendung automatischer Regeln für das Verschieben von Geräten zwischen Administrationsgruppen einzuschränken.

Wenn Sie automatische Regeln zum Verschieben von Geräten verwenden, kann dies zur Verbreitung von Richtlinien führen, die dem verschobenen Gerät mehr Berechtigungen gewähren, als das Gerät vor dem Verschieben besaß.

Darüber hinaus kann das Verschieben eines Client-Geräts in eine andere Administrationsgruppe zur Verbreitung von Richtlinieneinstellungen führen. Die Verteilung dieser Richtlinien an Gastgeräte und nicht vertrauenswürdige Geräte kann unerwünscht sein.

Diese Empfehlung gilt nicht für die einmalige erstmalige Zuordnung von Geräten zu Administrationsgruppen.

Sicherheitsanforderungen an Verteilungspunkte und Verbindungs-Gateways

Geräte mit installiertem Administrationsagenten können als Verteilungspunkt fungieren und die folgenden Funktionen ausführen:

- Vom Administrationsserver empfangene Updates und Installationspakete an die Client-Geräte innerhalb der Gruppe verteilen.
- Durchführen von Remote-Installationen von Drittanbieter-Programmen und Kaspersky-Anwendungen auf den Client-Geräten.
- Abfragen des Netzwerks, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden. Der Verteilungspunkt kann dieselben Methoden zur Geräteerkennung verwenden wie der Administrationsserver.

Das Platzieren von Verteilungspunkten im Netzwerk der Organisation kann für Folgendes verwendet werden:

- Entlastung des Administrationsservers
- Optimierung des Datenverkehrs
- Gewähren von Zugriff für den Administrationsserver auf Geräte, die sich an schwer erreichbaren Standorten des Unternehmensnetzwerks befinden

Unter Berücksichtigung der verfügbaren Funktionen empfehlen wir, alle Geräte, die als Verteilungspunkte fungieren, vor jeglicher Art von unbefugtem Zugriff (einschließlich physischem) zu schützen.

Einschränken der automatischen Zuweisung von Verteilungspunkten

Um die Administration zu vereinfachen und die Funktionsfähigkeit des Netzwerks zu erhalten, empfehlen wir die automatische Zuweisung von Verteilungspunkten. Für industrielle Netzwerke und kleine Netzwerke empfehlen wir jedoch, die automatische Zuweisung von Verteilungspunkten zu vermeiden. Das liegt darin begründet, da beispielsweise die privaten Informationen der Konten, die zum Anstoßen von Remote-Installationsaufgaben verwendet werden, mithilfe von Betriebssystem-Ressourcen an Verteilungspunkte übertragen werden können.

Für industrielle Netzwerke und kleine Netzwerke ist es möglich Geräten manuell die Rolle als Verteilungspunkt zuweisen.

Sie können auch den Bericht über die Aktivität der Verteilungspunkte anzeigen.

Sicherheitsanforderungen an die Geräte der Benutzer von Kaspersky Security Center

Für die Geräte der Benutzer von Kaspersky Security Center müssen besondere Sicherheitsanforderungen gelten. Es wird empfohlen, diese Geräte vor jeglicher Art von unbefugtem Zugriff (auch physisch) zu schützen:

Die Geräte der Benutzer von Kaspersky Security Center umfassen:

- Geräte, von denen sich Benutzer über einen Browser mit der Kaspersky Security Center Web Console verbinden.
- Geräte, von denen sich Benutzer anhand der MMC-basierten Verwaltungskonsole mit Kaspersky Security Center verbinden.
- Geräte, von denen sich Anwendungen, die mittels OpenAPI mit dem Administrationsserver kommunizieren, mit Kaspersky Security Center verbinden.

Sicherheitsanforderungen an Geräte mit installierter Kaspersky Security Center Web Console

Geräte mit installierter Kaspersky Security Center Web Console werden zur Verwaltung von Kaspersky Security Center verwendet. Es gelten daher besondere Sicherheitsanforderungen für diese Geräte. Es wird empfohlen, diese Geräte vor jeglicher Art von unbefugtem Zugriff (auch physisch) zu schützen.

Konfigurieren des Schutzes für verwaltete Programme

Verwaltete Richtlinien für Programme

Wir empfehlen das Erstellen einer Richtlinie für jede Art von verwendeten Anwendungen und Komponenten von Kaspersky Security Center (Administrationsagent, Kaspersky Endpoint Security für Windows, Kaspersky Endpoint Agent und weitere). Diese Richtlinie muss auf alle verwalteten Geräte (Stamm-Administrationsgruppe "Verwaltete Geräte") oder auf eine separate Gruppe, in die neue verwaltete Geräte gemäß den konfigurierten Verschiebungsregeln automatisch verschoben werden, angewendet werden.

Festlegen eines Kennworts zum Deaktivieren des Schutzes und Deinstallieren des Programms

Um zu verhindern, dass Eindringlinge die Kaspersky-Sicherheitsanwendungen deaktivieren, empfehlen wir dringend das Einrichten eines Kennwortschutzes für das Deaktivieren des Schutzes und für das Deinstallieren von Kaspersky-Sicherheitsanwendungen. Sie können ein Kennwort beispielsweise für Kaspersky Endpoint Security für Windows, Kaspersky Security für Windows Server, den Administrationsagenten und weitere Kaspersky-Anwendungen festlegen. Nachdem Sie den Kennwortschutz aktiviert haben, empfehlen wir, diese Einstellungen zu sperren, indem Sie das "Schloss" schließen.

Angeben des Kennworts für die manuelle Verbindung eines Client-Geräts mit dem Administrationsserver (Tool "klmover")

Mit dem Tool "klmover" können Sie ein Client-Gerät manuell mit dem Administrationsserver verbinden. Bei der Installation des Administrationsagenten auf dem Client-Gerät wird das Tool automatisch in den Installationsordner des Administrationsagenten kopiert.

Um zu verhindern, dass Angreifer Geräte aus dem Kontrollbereich Ihres Administrationsservers heraus verschieben können, wird es dringend empfohlen, für die Ausführung des Tools "klmover" den Kennwortschutz zu aktivieren. Um den Kennwortschutz zu aktivieren, wählen Sie in den Richtlinieneinstellungen des Administrationsagenten die Option **Deinstallationskennwort verwenden**.

Das Tool "klmover" erfordert lokale Administratorrechte. Für Geräte, die ohne lokale Administratorrechte betrieben werden, kann der Kennwortschutz für die Ausführung des Tools "klmover" ausgelassen werden.

Das Aktivieren der Option **Deinstallationskennwort verwenden** aktiviert ebenfalls den Kennwortschutz für das Cleaner-Tool (cleaner.exe).

Verwenden von Kaspersky Security Network

Wir empfehlen, in allen Richtlinien der verwalteten Programme und in den Eigenschaften des Administrationsservers die Verwendung von Kaspersky Security Network (KSN) zu aktivieren und die KSN-Erklärung zu akzeptieren. Wenn Sie den Administrationsserver aktualisieren, können Sie die aktualisierte KSN-Erklärung akzeptieren. In einigen Fällen können Sie KSN deaktivieren, z. B. wenn die Nutzung von Cloud-Diensten gesetzlich oder durch andere Vorschriften verboten ist.

Regelmäßiges Untersuchen verwalteter Geräte

Wir empfehlen, für alle Gerätegruppen eine Aufgabe zu erstellen, die regelmäßig eine vollständige Untersuchung der Geräte durchführt.

Suchen von neuen Geräten

Wir empfehlen, die Einstellungen der Gerätesuche ordnungsgemäß zu konfigurieren: Richten Sie die Integration mit Active Directory ein und geben Sie die IP-Adressbereiche für die Erkennung neuer Geräte an.

Aus Sicherheitsgründen können Sie die standardmäßige Administrationsgruppe verwenden, die alle neuen Geräte sowie die Standardrichtlinien enthält, die diese Gruppe betreffen.

Festlegen eines gemeinsamen Ordners

Wenn Sie den Administrationsserver auf einem Windows-Gerät mit einem vorhandenen freigegebenen Ordners bereitstellen (der beispielsweise zum Platzieren von Installationspaketen und zum Speichern aktualisierter Datenbanken verwendet wird), empfehlen wir sicherzustellen, dass für die Gruppe "Jeder" das Leserecht und für die Gruppe "KLAdmins" das Schreibrecht gewährt wurden.

Wartung des Administrationsservers

Anlegen eines Daten-Backups für den Administrationsservers

Ein Daten-Backup ermöglicht die Wiederherstellung der Daten des Administrationsservers ohne Datenverlust.

Standardmäßig wird nach der Installation des Administrationsservers automatisch eine Aufgabe zum Anlegen eines Daten-Backups erstellt und regelmäßig ausgeführt, wobei Sicherungen im entsprechenden Verzeichnis gespeichert werden.
Der Einstellungen der Aufgabe zum Anlegen eines Daten-Backups können wie folgt geändert werden:

- Die Frequenz des Datensicherung kann erhöht werden
- Es kann ein spezielles Verzeichnis zum Speichern von Kopien angegeben werden
- Kennwörter für Sicherungskopien können geändert werden

Wenn Sie Sicherungskopien in einem speziellen Verzeichnis ablegen, das sich vom Standardverzeichnis unterscheidet, empfehlen wir, die Zugriffskontrollliste (ACL) für dieses Verzeichnis einzuschränken. Die Konten für den Administrationsservers und für die Administrationsserver-Datenbank müssen Schreibzugriff auf dieses Verzeichnis haben.

Wartung des Administrationsservers

Durch die Wartung des Administrationsservers können Sie die Datenbankgröße reduzieren sowie die Leistungsfähigkeit und die Zuverlässigkeit des Programms verbessern. Es wird empfohlen, den Administrationsserver mindestens einmal pro Woche zu warten.

Die Wartung des Administrationsservers erfolgt mithilfe der entsprechenden Aufgaben. Bei der Wartung des Administrationsservers führt das Programm die folgenden Aktionen aus:

- Datenbanken auf Fehler überprüfen
- Datenbanken neu indizieren
- Datenbankstatistik aktualisieren
- Datenbank komprimieren (falls erforderlich)

Updates für das Betriebssystem und für Drittanbieter-Programme installieren

Wir empfehlen dringend, auf dem Gerät mit dem Administrationsserver regelmäßig Programm-Updates für das Betriebssystem und für die Drittanbieter-Programme zu installieren.

Client-Geräte benötigen keine ständige Verbindung zum Administrationsserver, daher ist es sicher, das Gerät mit dem Administrationsserver nach einer Update-Installation neu zu starten. Alle auf den Client-Geräten während einer Downtime des Administrationsservers registrierten Ereignisse werden nach Wiederherstellung der Verbindung an den Administrationsserver gesendet.

Ereignisübertragung an Systeme von Dritten

Überwachung und Berichterstattung

Um rechtzeitig auf Sicherheitsprobleme reagieren zu können, empfehlen wir, die Funktion Überwachung und Berichterstattung zu konfigurieren.

Ereignisse in SIEM-Systeme exportieren

Um Sicherheitsprobleme schnell zu erkennen und das Entstehen größerer Schäden zu vermeiden, empfehlen wir die Verwendung des Ereignisexports in ein SIEM-System.

E-Mail-Benachrichtigungen über Audit-Ereignisse

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Um rechtzeitig auf Notfälle reagieren zu können, empfehlen wir, den Administrationsserver so zu konfigurieren, dass er Benachrichtigungen über die von ihm veröffentlichten Audit-Ereignisse, kritischen Ereignisse, Fehlermeldungen und Warnungen sendet.

Da es sich bei diesen Ereignissen um interne System-Ereignisse handelt, ist mit einer geringen Anzahl von ihnen zu rechnen, was einem Versenden per Mail entgegenkommt.

Statistiken der Administrationsserver-Funktion

Für eine zeitnahe Reaktion auf Sicherheitsprobleme wird es empfohlen, das Senden von Statistiken der Administrationsserver-Funktion an Drittanbieter-Anwendungen zu konfigurieren, indem das Simple Network Management Protocol (SNMP) verwendet wird.

Sicherheitsempfehlungen für Drittanbieter-Informationssysteme

Sicherheitsempfehlungen für CIS-Benchmarks

Wenn Sie die vom Administrationsserver und vom Administrationsagenten unterstützten Versionen der Betriebssysteme, Virtualisierungsplattformen oder Datenbankserver einsetzen und diese Informationssysteme genauer anpassen möchten, empfehlen wir die bewährten Verfahren für Informationssicherheit des Center for Internet Security (CIS) (sofern vorhanden).

Das Center for Internet Security (CIS) ist eine gemeinnützige Organisation, die sich der Verbesserung der Sicherheit im Bereich der Informationstechnologie verschrieben hat. Insbesondere werden vom CIS Sicherheitsstandards wie die CIS Controls und CIS Benchmarks entwickelt und zur Verfügung gestellt. Diese Standards sind eine Reihe von Empfehlungen und Praktiken zur Gewährleistung der Sicherheit von Informationssystemen.

Das CIS-Portal enthält Empfehlungen für die Versionen der folgenden Informationssysteme, die vom Administrationsserver und vom Administrationsagenten unterstützt werden:

- Betriebssysteme aus folgenden Familien:
  - Windows für Desktops
  - Windows für Server
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware-Virtualisierungsplattformen
- Datenbankserver:
  - Microsoft SQL Server
  - MySQL

- MariaDB
- PostgreSQL

Sicherheitsempfehlungen für das Betriebssystem Astra Linux

Wenn Sie das Betriebssystem Astra Linux verwenden, sollten Sie die Sicherheitsempfehlungen befolgen, die im Red Book der entsprechenden Version von Astra Linux (auf Russisch) beschrieben sind.

Sicherheitsempfehlungen für das Betriebssystem RED OS

Wenn Sie das Betriebssystem RED OS verwenden, sollten Sie die in der offiziellen Dokumentation zu RED OS beschriebenen Sicherheitsempfehlungen des Administratorhandbuchs befolgen.

Empfehlungen für die Verwendung von Kaspersky-Sicherheitsanwendungen

Verwendung des KLAdmin-Kennworts in Kaspersky Endpoint Security für Windows

Es können sich mehrere Benutzer mit unterschiedlichen Computerkenntnissen ein Gerät teilen, auf dem Kaspersky Endpoint Security für Windows installiert ist. Wenn Benutzer einen uneingeschränkten Zugang zu Kaspersky Endpoint Security für Windows und dessen Einstellungen haben, kann dies das allgemeine Schutzniveau des Geräts verringern. Der Kennwortschutz ermöglicht es Ihnen, den Zugriff für Benutzer auf Kaspersky Endpoint Security für Windows entsprechend der ihnen gewährten Berechtigungen (etwa das Recht, die Anwendung zu beenden) einzuschränken.

Eine der Möglichkeiten, den Zugriff auf Kaspersky Endpoint Security für Windows und seine Einstellungen einzuschränken, besteht darin, ein KLAdmin-Konto zu verwenden. Das KLAdmin-Konto ist ein Administratorkonto mit uneingeschränktem Zugriff auf Kaspersky Endpoint Security für Windows. Das Benutzerkonto "KLAdmin" ist dazu berechtigt, sämtliche kennwortgeschützten Vorgänge in Kaspersky Endpoint Security für Windows auszuführen. Die Berechtigungen für das KLAdmin-Konto können nicht widerrufen werden. Sie können das Kennwort für das KLAdmin-Konto in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows festlegen. Der Administrator von Kaspersky Endpoint Security für Windows ist voll verantwortlich für die sichere Verwendung des Kennworts für das KLAdmin-Konto. Wenn Ihre Organisation eine eigene Kennwort Richtlinie besitzt, folgen Sie den Anweisungen dieser Richtlinie.

Unsere Empfehlungen für den Schutz einer Organisation vor dem Diebstahl des KLAdmin-Kennworts lauten wie folgt:

- **Allgemeine Anforderungen**

  Verwenden Sie weder den gesamten Kontonamen noch einen Teil des Namens als Kennwort.

- **Minimale Länge des Kennworts**

  Das Kennwort muss mindestens 10 Zeichen lang sein.

- **Obligatorische Zeichenkategorien**

  Legen Sie ein komplexes Kennwort mit Zeichen aus unterschiedlichen Kategorien fest: Klein- und Großbuchstaben, Ziffern und Sonderzeichen.

- **Gültigkeitsdauer des Kennworts**

  Legen Sie für das Kennwort eine Gültigkeitsdauer von mindestens 90 Tagen fest. Ein neues Kennwort darf nicht mit einem der letzten 24 Kennwörter übereinstimmen.

Vorbereitung der Bereitstellung

In diesem Abschnitt werden Schritte beschrieben, die Sie unternehmen müssen, bevor Sie Kaspersky Security Center verteilen.

Planung der Bereitstellung für Kaspersky Security Center

Dieser Abschnitt informiert darüber, wie die Komponenten von Kaspersky Security Center in einem Unternehmensnetzwerk, abhängig von den folgenden Faktoren, optimal bereitgestellt werden:

- Gesamtzahl der Geräte
- Existenz von Unternehmens- oder geographisch isolierten Abteilungen (Büros, Filialen)
- Existenz von isolierten Netzwerken, die über enge Kanäle verbunden sind
- Notwendigkeit des Zugriffs auf den Administrationsserver über das Internet

Typische Vorgehensweisen der Bereitstellung

In diesem Abschnitt werden typische Methoden zur Bereitstellung des Schutzsystems mithilfe von Kaspersky Security Center in einem Unternehmensnetzwerk beschrieben.

Das System muss vor unbefugten Zugriffen aller Art geschützt werden. Es wird empfohlen, vor der Installation des Programms auf Ihrem Gerät alle verfügbaren Updates des Betriebssystems zu installieren und die Administrationsserver sowie die Verteilungspunkte vor physischem Zugriff zu schützen.

Sie können Antiviren-Programme im Netzwerk eines Unternehmens mithilfe von Kaspersky Security Center bereitstellen, indem Sie folgende Vorgehensweisen zur Bereitstellung verwenden:

- Bereitstellung der Antiviren-Programme über Kaspersky Security Center auf eine der folgenden Arten:
  - Mittels der Verwaltungskonsole.
  - Mittels der Kaspersky Security Center Web Console

  Die Installation von Kaspersky-Anwendungen auf Client-Geräten und die Verbindung von Client-Geräten mit dem Administrationsserver erfolgt automatisch mithilfe von Kaspersky Security Center.

  Die wichtigste Vorgehensweise zur Bereitstellung ist die Verteilung des Antiviren-Schutzes über die Verwaltungskonsole. Kaspersky Security Center Web Console ermöglicht die Installation von Kaspersky-Anwendungen über einen Webbrowser.
- Manuelle Bereitstellung der Antiviren-Programme mithilfe autonomer Installationspakete, die in Kaspersky Security Center erstellt wurden

Die Installation von Kaspersky-Anwendungen auf den Client-Geräten und dem Administrator-Arbeitsplatz erfolgt manuell. Die Einstellungen für die Verbindung der Client-Geräte mit dem Administrationsserver werden bei der Installation des Administrationsagenten vorgegeben.

Diese Variante der Bereitstellungwird empfohlen, wenn keine Remote-Installation möglich ist.

Außerdem ermöglicht Kaspersky Security Center die Verteilung von Antiviren-Programmen mithilfe von Gruppenrichtlinien des Active Directory®.

Informationen über die Planung der Verteilung von Kaspersky Security Center in einem Unternehmensnetzwerk

Ein Administrationsserver kann nicht mehr als 100.000 Geräte verwalten. Wenn die Gesamtzahl der Geräte im Unternehmensnetzwerk 100.000 überschreitet, müssen im Unternehmensnetzwerk mehrere Administrationsserver verteilt werden, die zur einfacheren zentralen Verwaltung in einer Hierarchie zusammengefasst sind.

Wenn es in der Zusammensetzung des Unternehmens große, geographisch voneinander entfernte Büros (Filialen) mit eigenen Administratoren gibt, es ist zweckmäßig, in diesen Büros Administrationsserver zu implementieren. Andernfalls müssen solche Büros wie isolierte Netzwerke betrachtet werden, die über Kanäle mit niedrigem Durchsatz verbunden sind; s. Abschnitt "Standard-Konfiguration: Wenige größere Büros werden jeweils von eigenen Administratoren verwaltet".

Bei Vorhandensein von isolierten Netzwerken, die über enge Kanäle verbunden sind, müssen zwecks Optimierung des Datenverkehrs in solchen Netzwerken ein oder mehrere Administrationsagenten als Verteilungspunkte bestimmt werden (s. Tabelle zur Berechnung der Anzahl der Verteilungspunkte). In diesem Fall erhalten alle Geräte in einem isolierten Netzwerk die Updates von solchen "lokalen Update-Zentren". Die Verteilungspunkte können die Updates sowohl vom Administrationsserver (Standardszenario) als auch von den im Internet verfügbaren Servern von Kaspersky herunterladen (siehe auch Abschnitt Typische Konfiguration: Mehrere kleine Remote-Büros).

Im Abschnitt Typische Konfigurationen von Kaspersky Security Center erhalten Sie ausführliche Beschreibungen der typischen Konfigurationen von Kaspersky Security Center. Bei der Planung der Bereitstellung muss je nach der Struktur des Unternehmens, die am geeignetste typische Konfiguration ausgewählt werden.

Bei der Planung der Bereitstellung muss die Notwendigkeit zur Angabe des speziellen Zertifikates X.509 für den Administrationsserver in Betracht gezogen werden. Die Angabe des Zertifikates X.509 für den Administrationsserver kann in folgenden Fällen (unvollständige Liste) zweckmäßig sein:

- Zur Untersuchung des SSL-Datenverkehres mittels SSL Termination Proxy oder zur Nutzung von Reverse Proxy
- Zur Integration der PKI-Infrastruktur (PKI) des Unternehmens
- Zur Angabe der gewünschten Werte für die Felder des Zertifikats
- Zur Gewährleistung der erwünschten Verschlüsselungsstärke des Zertifikats

Struktur des Schutzes im Unternehmen auswählen

Die Auswahl einer Struktur für den Schutz im Unternehmen wird durch folgende Faktoren bestimmt:

- Netztopologie des Unternehmens
- Organisationsstruktur

- Anzahl der für den Antiviren-Schutz zuständigen Mitarbeiter und deren Aufgabenverteilung
- Hardwareressourcen, die für die Installation von Antiviren-Schutzkomponenten zur Verfügung gestellt werden können
- Bandbreite der Kommunikationskanäle, die für den Einsatz der Antiviren-Schutzkomponenten im Netzwerk des Unternehmens zur Verfügung gestellt werden können
- Annehmbare Zeit für die Durchführung von kritischen administrativen Vorgängen im Netzwerk des Unternehmens Zu kritischen administrativen Vorgängen gehören zum Beispiel die Verbreitung von Updates der Antiviren-Datenbanken und die Veränderung von Richtlinien für die Client-Geräte

Bei der Wahl der Antiviren-Schutzstruktur empfiehlt es sich, zunächst die vorhandenen Netzwerk- und Hardwareressourcen zu bestimmen, die sich für das zentrale Virenschutz-System verwenden lassen.

Für die Analyse der Netzwerk- und Hardwareinfrastruktur wird die folgende Vorgehensweise empfohlen:

1. Legen Sie die folgenden Einstellungen für das Netzwerk fest, in dem die Antiviren-Programme verteilt werden sollen:
   - Anzahl der Netzwerksegmente.
   - Geschwindigkeit der Kommunikationskanäle zwischen den einzelnen Netzwerksegmenten.
   - Anzahl der verwalteten Geräte in jedem Netzwerksegment.
   - Bandbreite aller Kommunikationskanäle, die für den Antiviren-Schutz zur Verfügung gestellt werden kann.
2. Definieren Sie die zulässige Dauer für die Durchführung wichtiger administrativer Operationen für alle verwalteten Geräte.
3. Analyse der Informationen aus den Punkten 1 und 2, sowie der Daten der Belastungstests des Administrationssystems. Beantworten Sie anhand der durchgeführten Analyse folgende Fragen:
   - Können alle Clients mit einem einzigen Administrationsserver bedient werden oder ist eine Hierarchie von Administrationsservern erforderlich?
   - Welche Hardwarekonfiguration der Administrationsserver ist nötig, um alle Clients in der in Punkt 2 festgelegten Zeit zu bedienen?
   - Ist eine Verwendung von Verteilungspunkten nötig, um die Auslastung der Kommunikationskanäle zu verringern?

Nachdem Sie die oben in Punkt 3 angeführten Fragen beantwortet haben, können Sie denkbare Antiviren-Schutzstrukturen für das Unternehmen zusammenstellen.

Im Netzwerk des Unternehmens kann eine der folgenden typischen Antiviren-Schutzstrukturen verwendet werden:

- Ein einziger Administrationsserver. Alle Client-Geräte sind mit einem einzigen Administrationsserver verbunden. Der Administrationsserver agiert als Verteilungspunkt.
- Ein einziger Administrationsserver mit Verteilungspunkten. Alle Client-Geräte sind mit einem einzigen Administrationsserver verbunden. Im Netzwerk sind Client-Geräte zur Verfügung gestellt, die als Verteilungspunkte agieren.

- Administrationsserver-Hierarchie. Für jedes Netzwerksegment wird ein separater Administrationsserver zur Verfügung gestellt, der in die allgemeine Hierarchie der Administrationsserver eingeschlossen ist. Der primäre Administrationsserver agiert als Verteilungspunkt.

- Administrationsserver-Hierarchie mit Verteilungspunkten. Für jedes Netzwerksegment wird ein separater Administrationsserver zur Verfügung gestellt, der in die allgemeine Hierarchie der Administrationsserver eingeschlossen ist. Im Netzwerk sind Client-Geräte zur Verfügung gestellt, die als Verteilungspunkte agieren.

Typische Konfigurationen von Kaspersky Security Center

In diesem Abschnitt werden die folgenden typischen Konfigurationen für die Verteilung der Komponenten von Kaspersky Security Center im Unternehmensnetzwerk beschrieben:

- Einzelbüro
- Mehrere große, geographisch verteilte Büros mit eigenen Administratoren
- Eine Menge kleine, geographisch verteilte Büros

Typische Konfiguration: Einzelbüro

Im Netzwerk des Unternehmens können ein oder mehrere Administrationsserver vorhanden sein. Die Anzahl der Administrationsserver kann sowohl ausgehend von der vorhandenen verfügbaren Hardware als auch in Abhängigkeit von der Gesamtmenge der verwalteten Geräte ausgewählt werden.

Ein Administrationsserver kann bis zu 100.000 Geräte verwalten. Die Möglichkeit einer Erhöhung der Anzahl der verwalteten Geräte in nächster Zukunft muss berücksichtigt werden: es kann sich als wünschenswert erweisen, eine etwas kleinere Anzahl von Geräten mit einem Administrationsserver zu verbinden.

Die Administrationsserver können sich sowohl im internen Netzwerk als auch in der demilitarisierten Zone befinden, abhängig davon, ob ein Zugriff auf die Administrationsserver aus dem Internet erforderlich ist.

Wenn es mehrere Server gibt, ist es empfehlenswert, sie in einer Hierarchie zusammenzufassen. Durch Verwendung einer Hierarchie der Administrationsserver können Sie das Duplizieren von Richtlinien und Aufgaben vermeiden, und mit allen verwalteten Geräte arbeiten, als ob sie von einem einzigen Administrationsserver verwaltet würden (z. B. Geräte suchen, Geräteauswahlen erstellen und Berichte erstellen).

Typische Konfiguration: Mehrere größere Büros mit eigenen Administratoren

Für ein Unternehmen, das mehrere große Büros an unterschiedlichen Orten hat, sollten Sie die Option berücksichtigen, die Administrationsserver in jedem dieser Büros zu verteilen. In jedem Büro können ein oder mehrere Administrationsserver verteilt werden, abhängig von der Anzahl der Client-Geräte und der verfügbaren Hardware. In diesem Fall kann jedes Büros als Typische Einzelbüro-Konfiguration betrachtet werden. Um die Verwaltung zu vereinfachen, wird empfohlen, alle Administrationsserver in einer Hierarchie (ggf. mit mehreren Ebenen) zusammenzufassen.

Wenn einige Mitarbeiter mit ihren Geräten (Laptops) zwischen den Büros wechseln, können Sie Verbindungsprofile für den Administrationsagenten in der Richtlinie des Administrationsagenten erstellen. Die Verbindungsprofile des Administrationsagenten werden nur für Geräte mit Windows oder macOS unterstützt.

Typische Konfiguration: Mehrere kleine Remote-Büros

Diese Standardkonfiguration ist vorgesehen für eine Unternehmenszentrale und zahlreiche kleine Remote-Büros, die über das Internet mit der Zentrale kommunizieren können. Die einzelnen Remote-Büros können sich hinter einer Netzwerkadressübersetzung (NAT) befinden. Das heißt, eine Verbindung zwischen zwei Remote-Büro ist nicht möglich, da die Büros voneinander isoliert sind.

In der Unternehmenszentrale muss ein Administrationsserver bereitgestellt werden, und ein oder mehrere Verteilungspunkte müssen allen übrigen Büros zugewiesen werden. Wenn eine Verbindung zwischen den Büros über das Internet hergestellt wird, kann es sinnvoll sein, für die Verteilungspunkte eine *Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte* zu erstellen, damit die Verteilungspunkte die Updates nicht vom Administrationsserver, sondern direkt von den Kaspersky-Servern oder lokalen oder Netzwerkordnern herunterladen.

Wenn im Remote-Büro ein Teil der Geräte keinen direkten Zugriff zum Administrationsserver hat (beispielsweise wenn der Zugriff auf den Administrationsserver durch das Internet erfolgt, aber nicht alle Geräte über Internetzugang verfügen), müssen die Verteilungspunkte in den Gateway-Modus (Verbindungs-Gateway) umgeschaltet werden. In diesem Fall werden die Administrationsagenten auf den Geräten im Remote-Büro (zwecks Synchronisierung) nicht direkt, sondern über ein Gateway mit dem Administrationsserver verbunden.

Da der Administrationsserver das Netzwerk im Remote-Büro aller Wahrscheinlichkeit nach nicht abfragen kann, ist es sinnvoll, das Ausführen dieser Funktion auf einen der Verteilungspunkte zu übertragen.

Der Administrationsserver kann an verwaltete Geräte, welche sich im Remote-Büro hinter NAT befinden, keine Benachrichtigung an den UDP-Port 15000 senden. Um dieses Problem zu beheben, können Sie in den Eigenschaften der Geräte, die als Verteilungspunkte dienen, den Modus zur ständigen Verbindung mit dem Administrationsserver (Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**) aktivieren. Dieser Modus ist verfügbar, wenn die Gesamtanzahl der Verteilungspunkte 300 nicht überschreitet. Verwenden Sie Push-Server, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht. Weitere Informationen finden Sie im folgenden Thema: Verteilungspunkt als Push-Server verwenden.

DBMS für den Administrationsserver auswählen

Bei der Auswahl des DBMS, das vom Administrationsserver verwendet wird, muss von der Anzahl der Geräte ausgegangen werden, die der Administrationsserver betreut.

In der nachfolgenden Tabelle sind die zulässigen DBMS-Varianten und deren Empfehlungen und Einschränkungen zur Verwendung aufgeführt.

Empfehlungen und Einschränkungen der DBMSs

DBMS	Empfehlungen und Einschränkungen
SQL Server Express Edition 2016 und höher.	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 10.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Sie können die maximale Anzahl an Ereignissen in der Ereignisverwaltung begrenzen, um ein Überlaufen der Datenbank zu verhindern. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank. Die gleichzeitige Verwendung des DBMS von SQL Server Express Edition durch den Administrationsserver und eine weitere Anwendung ist unzulässig. Die Microsoft SQL Express-Datenbank wird für die Aufgabe **Windows-Updates synchronisieren** nicht unterstützt.
SQL Server Edition (keine Express Edition), 2016 und höher, lokale Bereitstellung	Keine Einschränkungen.
SQL Server Edition (keine Express Edition), 2016 und höher, Remote-Bereitstellung	Nur gültig, wenn sich beide Geräte in derselben Windows®-Domäne befinden. Wenn die Domänen unterschiedlich sind, muss zwischen ihnen eine wechselseitige Vertrauensstellung hergestellt werden.

DBMS	Empfehlungen und Einschränkungen
MySQL 5.5, 5.6 oder 5.7 (die MySQL Versionen 5.5.1, 5.5.2, 5.5.3, 5.5.4 und 5.5.5 werden nicht mehr unterstützt), lokale oder Remote-Bereitstellung	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 10.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.
MySQL 8.0.20 oder höher, lokale oder Remote-Bereitstellung	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.
MariaDB (siehe unterstützte Versionen), lokale oder Remote-Bereitstellung	Verwenden Sie dieses DBMS, wenn Sie einen Administrationsserver für bis zu 20.000 Geräte verwenden möchten. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.
PostgreSQL, Postgres Pro (siehe unterstützte Versionen)	Verwenden Sie eins dieser DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.

Wenn Sie MSSQL 2019 auswählen, müssen Sie den kumulativen Patch CU12 oder höher verwenden. Dadurch können Sie auftretende Fehler und eine Systemüberlastung vermeiden.

Den kumulativen Patches CU12 bei Verwendung von SQL Server 2019 als DBMS anwenden

Wenn Sie SQL Server 2019 als DBMS verwenden und nicht über den kumulativen Patch CU12 oder höher verfügen, installieren Sie diesen. Dadurch vermeiden Sie Fehler wie "Der Systemspeicher im Ressourcenpool 'internal' reicht nicht aus, um diese Abfrage auszuführen".

Führen Sie nach der Installation von Kaspersky Security Center die folgenden Schritte aus:

1. Mithilfe von SQL Management Studio eine Verbindung mit SQL Server herstellen.
2. Folgende Befehle ausführen (wenn Sie einen anderen Namen für die Datenbank gewählt haben, verwenden Sie diesen Namen anstelle von "KAV"):

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Den Dienst von SQL Server 2019 neu starten.

MariaDB x64-Server für die Arbeit mit Kaspersky Security Center 15.1 konfigurieren

Um den Server von MariaDB x64 erfolgreich für die Arbeit mit Kaspersky Security Center zu konfigurieren, müssen Sie mit Ausnahme der in diesem Artikel angegebenen Serverparameter die standardmäßigen Serverparameter verwenden.

Kaspersky Security Center 15.1 unterstützt das DBMS MariaDB. Weitere Informationen zu unterstützten Versionen von MariaDB finden Sie im Abschnitt Hardware- und Softwarevoraussetzungen.

Wenn Sie MariaDB als DBMS für Kaspersky Security Center verwenden, aktivieren Sie die Unterstützung für InnoDB und MEMORY-Speicher sowie für die Codierungen UTF-8 und UCS-2.

Empfohlene Einstellungen für die Datei my.ini

Um die Datei my.ini zu konfigurieren:

1. Öffnen Sie die Datei my.ini in einem Texteditor.

2. Fügen Sie in der Datei my.ini im Abschnitt `[mysqld]` die folgenden Zeilen hinzu:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< der tatsächliche Wert muss nicht weniger als 80 % der Größe der erwarteten KAV-Datenbank sein >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   Der Wert von `innodb_buffer_pool_size` muss mindestens 80 Prozent der erwarteten KAV-Datenbankgröße betragen. Beachten Sie, dass der angegebene Speicher beim Start des Servers zugewiesen wird. Wenn die Datenbankgröße kleiner als der angegebene Buffer-Wert ist, wird nur der erforderliche Speicher zugewiesen. Wenn Sie MariaDB 10.4.3 oder älter verwenden, ist die tatsächliche Größe des zugewiesenen Speichers etwa 10 Prozent größer als der angegebene Buffer-Wert.

   Es wird empfohlen, den Parameterwert `innodb_flush_log_at_trx_commit=0` zu verwenden, da die Werte "1" oder "2" die Geschwindigkeit von MariaDB negativ beeinflussen. Stellen Sie sicher, dass der Parameter `innodb_file_per_table` auf `1` gesetzt ist.

   Geben Sie für MariaDB 10.1 zusätzlich die folgenden Zeilen im "[mysqld]"-Abschnitt ein:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

Geben Sie für MariaDB 10.6 zusätzlich die folgenden Zeilen im "[mysqld]"-Abschnitt ein:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Standardmäßig sind die Optimierungs-Add-ons `join_cache_incremental`, `join_cache_hashed`, und `join_cache_bka` aktiviert. Wenn diese Add-ons nicht aktiviert sind, müssen Sie diese aktivieren.

Um zu überprüfen, ob die Optimierungs-Add-ons aktiviert sind:

1. Führen Sie in der MariaDB-Client-Konsole den folgenden Befehl aus:

   ```
   SELECT @@optimizer_switch;
   ```

2. Überprüfen Sie, ob die Ausgabe die folgenden Zeilen enthält:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Wenn diese Zeilen vorhanden sind und den Wert `on` besitzen, sind die Optimierungs-Add-ons aktiviert.

   Falls diese Zeilen fehlen oder den Wert `off` besitzen:

   1. Öffnen Sie die Datei my.ini in einem Texteditor.

   2. Fügen Sie in der Datei my.ini im Abschnitt `[mysqld]` die folgenden Zeilen hinzu:

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

Die Add-ons `join_cache_incremental`, `join_cache_hash` und `join_cache_bka` sind aktiviert.

MySQL x64-Server für die Arbeit mit Kaspersky Security Center 15.1 konfigurieren

Um den Server von MySQL x64 erfolgreich für die Arbeit mit Kaspersky Security Center einzurichten, müssen Sie mit Ausnahme der in diesem Artikel angegebenen Serverparameter die standardmäßigen Serverparameter verwenden.

Wenn Sie MySQL als DBMS für Kaspersky Security Center verwenden, aktivieren Sie die Unterstützung für InnoDB und MEMORY-Speicher sowie für die Codierungen UTF-8 und UCS-2.

Empfohlene Einstellungen für die Datei my.ini

Um die Datei my.ini zu konfigurieren:

1. Öffnen Sie die Datei my.ini in einem Texteditor.

2. Fügen Sie in der Datei my.ini im Abschnitt `[mysqld]` die folgenden Zeilen hinzu:

   ```
   sort_buffer_size=10M
   join_buffer_size=20M
   tmp_table_size=600M
   max_heap_table_size=600M
   key_buffer_size=200M
   innodb_buffer_pool_size=< der tatsächliche Wert muss nicht weniger als 80 % der Größe der erwarteten KAV-Datenbank sein >
   ```

```
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (in den meisten Fällen nutzt der Server kleine
Transaktionen)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Beachten Sie, dass der für den Wert `innodb_buffer_pool_size` angegebene Speicher beim Start des Servers zugewiesen wird. Wenn die Datenbankgröße kleiner als der angegebene Buffer-Wert ist, wird nur der erforderliche Speicher zugewiesen. Die tatsächliche Größe des zugewiesenen Speichers ist ungefähr 10 Prozent größer als der angegebene Buffer-Wert. Weitere Informationen entnehmen Sie der Dokumentation zu MySQL.

Es wird empfohlen, den Parameterwert `innodb_flush_log_at_trx_commit = 0` zu verwenden, da die Werte "1" oder "2" die Geschwindigkeit von MySQL negativ beeinflussen. Stellen Sie sicher, dass der Parameter `innodb_file_per_table` auf `1` gesetzt ist.

PostgresSQL- oder Postgres Pro-Server für die Arbeit mit Kaspersky Security Center 15.1 konfigurieren

Um den Server von PostgreSQL oder Postgres Pro erfolgreich für die Arbeit mit Kaspersky Security Center einzurichten, müssen Sie mit Ausnahme der in diesem Artikel angegebenen Serverparameter die standardmäßigen Serverparameter verwenden.

Kaspersky Security Center 15.1 unterstützt PostgreSQL und Postgres Pro als DBMS. Wenn Sie eines dieser DBMS verwenden, sollten Sie die Parameter des entsprechenden DBMS-Servers konfigurieren, um die Ausführung des DBMS in Bezug auf Kaspersky Security Center zu optimieren.

Der Standardpfad zur Konfigurationsdatei lautet: `C:\Program Files\PostgreSQL\<VERSION>\data\postgresql.conf`

Empfohlene Parameter für PostgreSQL und Postgres Pro:

- `max_connections = 151`
- `shared_buffers = N`

  N = 25 Prozent des RAM-Werts des Geräts, auf dem das DBMS installiert ist. Wenn der Arbeitsspeicher weniger als 1 GB beträgt, belassen Sie den Standardwert.
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `maintenance_work_mem = 128MB`
- `max_stack_depth = 2MB`
- `max_parallel_workers_per_gather = 0`
- `standard_conforming_strings = on`

Wenn Sie Postgres Pro 15.7 oder Postgres Pro 15.7.1 verwenden, deaktivieren Sie den Parameter `enable_compound_index_stats`:

```
enable_compound_index_stats = off
```

Laden Sie die Konfiguration neu oder starten Sie den DBMS-Server neu, nachdem Sie die Konfigurationsdatei aktualisiert haben.

Weitere Informationen zu den Serverparametern von PostgreSQL und Postgres Pro und zu deren Konfiguration finden Sie in der entsprechenden DBMS-Dokumentation.

Weitere Informationen zum Erstellen und Konfigurieren von Konten für PostgreSQL und Postgres Pro finden Sie im folgenden Thema: Benutzerkonten für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren.

Unterstützung für hochverfügbare Cluster

Hochverfügbare PostgreSQL-Cluster werden mit den folgenden Einstellungen unterstützt:

- Replikationstyp: synchron
- Minimale Anzahl von Knoten: 3
- Maximale Anzahl von Knoten: 15

Um diese Funktion zu verwenden, müssen Sie den folgenden Befehl ausführen, um das Flag KLCS_FF_SUPPORT_POSTGRES_FAIILOVER zu aktivieren:

```
sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv ".core/.independent" -s klcsff -n
KLCS_FF_SUPPORT_POSTGRES_FAIILOVER -t d -v 1
```

Die Postgres-Rolle, die vom Server für den DBMS-Zugriff verwendet wird, muss über Berechtigungen zum Lesen der folgenden Views verfügen (standardmäßig aktiviert):

- pg_stat_replication
- pg_stat_wal_receiver

Mobile Geräte mit installiertem Kaspersky Endpoint Security für Android verwalten

Die Verwaltung von mobilen Geräten mit installierter App Kaspersky Endpoint Security für Android™ (im Weiteren KES-Geräte) erfolgt mithilfe des Administrationsservers. Kaspersky Security Center unterstützt die folgenden Funktionen zur Verwaltung von KES-Geräten:

- Arbeit mit mobilen Geräten und den Client-Geräten:
  - Zugehörigkeit zu Administrationsgruppen
  - Überwachung, z. B. Anzeigen von Statuswerten, Ereignissen und Berichten
  - Änderung der lokalen Einstellungen und Festlegung der Richtlinie für die App Kaspersky Endpoint Security für Android

- Zentralisierter Versand von Befehlen
- Remote-Installation der Pakete mit mobilen Anwendungen

Der Administrationsserver verwaltet KES-Geräte über TLS, TCP-Port 13292.

Internetzugriff für den Administrationsserver bereitstellen

Für die folgenden Fälle muss der Zugriff auf den Administrationsserver aus dem Internet gewährt werden:

- Regelmäßiges Aktualisieren der Datenbanken, Softwaremodule und Programme von Kaspersky
- Aktualisieren von Drittanbieter-Programmen

  Standardmäßig ist für den Administrationsserver keine Internetverbindung erforderlich, um Updates für Software von Microsoft auf den verwalteten Geräten zu installieren. Beispielsweise können die verwalteten Geräte die Updates für Software von Microsoft direkt von den Microsoft Update-Servern oder von einem Windows Server mit im Unternehmensnetzwerk bereitgestelltem Microsoft Windows Server Update Services (WSUS) herunterladen. In den folgenden Fällen muss der Administrationsserver mit dem Internet verbunden sein:

  - Wenn Sie Administrationsserver als WSUS-Server verwenden
  - So installieren Sie Updates für Drittanbieter-Programme, die keine Software von Microsoft darstellen
- Schließen von Schwachstellen in Programmen von Drittanbietern

  Damit der Administrationsserver die folgenden Aufgaben ausführen kann, ist eine Internetverbindung erforderlich:

  - Erstellen einer Liste empfohlener Korrekturen für Schwachstellen in Software von Microsoft. Die Liste wird von Kaspersky-Spezialisten erstellt und regelmäßig aktualisiert.
  - Schwachstellen Drittanbieter-Programmen beheben, keine Software von Microsoft darstellen.
- Für die Verwaltung von Geräten (Laptops) der eigenständigen Benutzer
- Für die Verwaltung von Geräten, die sich in Remote-Büros befinden
- Bei der Interaktion mit primären oder sekundären Administrationsservern, die sich in Remote-Büros befinden
- Zur Verwaltung von mobilen Geräten

In diesem Abschnitt werden die typischen Methoden zur Gewährleistung des Zugriffs auf den Administrationsserver über das Internet beschrieben. Für alle Fälle der Bereitstellung des Zugriffes auf den Administrationsserver über das Internet kann es erforderlich sein, für den Administrationsserver ein spezielles Zertifikat festzulegen.

Internetzugriff: Administrationsserver in einem lokalen Netzwerk

Wenn sich der Administrationsserver im internen Netzwerk des Unternehmens befindet, kann es hilfreich sein, den TCP-Port 13000 des Administrationsservers mithilfe der Portweiterleitung von außen erreichbar zu machen. Wenn die Verwaltung mobiler Geräte erforderlich ist, kann es hilfreich sein, den Port 13292 TCP erreichbar zu machen.

Zugriff aus dem Internet: Administrationsserver in der demilitarisierten Zone

Wenn sich der Administrationsserver in der demilitarisierten Zone des Unternehmensnetzwerks befindet, hat er keinen Zugriff auf das interne Netzwerk des Unternehmens. Daraus ergeben sich die folgenden Einschränkungen:

- Der Administrationsserver kann neue Geräte nicht selbstständig finden.
- Der Administrationsserver kann die erstmalige Bereitstellung des Administrationsagenten nicht mittels erzwungener Installation auf den Geräten des internen Netzwerks des Unternehmens ausführen.

Es handelt sich nur um die erstmalige Installation des Administrationsagenten. Die nachfolgenden Updates der Version des Administrationsagenten oder die Installation der Sicherheitsanwendungen können bereits vom Administrationsserver ausgeführt werden. Jedoch kann die erstmalige Bereitstellung der Administrationsagenten mit anderen Mitteln, beispielsweise mithilfe der Gruppenrichtlinien von Microsoft® Active Directory® ausgeführt werden.

- Der Administrationsserver kann über den UDP-Port 15000 keine Benachrichtigungen an die verwalteten Geräte senden. Dies ist nicht kritisch für die Funktionalität von Kaspersky Security Center.
- Der Administrationsserver kann keine Abfrage von Active Directory durchführen. Die Ergebnisse einer Active Directory-Abfrage sind allerdings in der Mehrzahl der Szenarien nicht erforderlich.

Wenn die oben beschriebenen Beschränkungen kritisch sind, können sie mithilfe von Verteilungspunkten aufgehoben werden, die sich im Unternehmensnetzwerk befinden:

- Für das Ausführen der erstmaligen Bereitstellung auf Geräten ohne Administrationsagenten muss der Administrationsagent vorläufig auf einem der Geräte installiert und dieses Gerät als Verteilungspunkt bestimmt werden. Daraufhin wird die erstmalige Installation des Administrationsagenten auf den übrigen Geräten vom Administrationsserver durch diesen Verteilungspunkt ausgeführt.
- Für das Finden neuer Geräte im internen Netzwerk des Unternehmens und für die Abfrage von Active Directory müssen auf einem der Verteilungspunkte die erwünschten Methoden zur Gerätesuche aktiviert werden.

Um sicherzustellen, dass Benachrichtigungen an den UDP-Port 15000 erfolgreich auf verwalteten Geräten gesendet werden, die sich im internen Unternehmensnetzwerk befinden, müssen Sie das gesamte Unternehmensnetzwerk mit Verteilungspunkten abdecken. Aktivieren Sie in den Eigenschaften der zugewiesenen Verteilungspunkte das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**. Dadurch stellt der Administrationsserver eine kontinuierliche Verbindung zu den Verteilungspunkten her und die Verteilungspunkte können Benachrichtigungen an den UDP-Port 15000 auf den Geräten senden, die sich im internen Unternehmensnetzwerk befinden (das trifft auf IPv4- oder IPv6-Netzwerke zu).

Zugriff aus dem Internet: Administrationsagent als Verbindungs-Gateway in der demilitarisierten Zone

Der Administrationsserver kann sich im internen Netzwerk der Organisation befinden, in dessen DMZ sich wiederum ein Gerät befindet, auf dem ein Administrationsagent als rückwärtsgerichtetes Verbindungs-Gateway ausgeführt wird (der Administrationsserver stellt eine Verbindung zum Administrationsagenten her). In diesem Fall müssen für die Organisation des Zugriffs aus dem Internet die folgenden Bedingungen erfüllt werden:

- Der Administrationsagent muss auf dem Gerät installiert werden, welches sich in der DMZ befindet. Wählen Sie bei der Installation des Administrationsagenten im Fenster **Verbindungs-Gateway** des Installationsassistenten den Punkt **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden** aus.

- Das Gerät mit dem installierten Verbindungs-Gateway muss als Verteilungspunkt hinzugefügt werden. Wenn Sie das Verbindungs-Gateway in dem Fenster **Verteilungspunkt hinzufügen** angeben, wählen Sie die Option **Auswählen → Verbindungs-Gateway in DMZ mittels Adresse hinzufügen**.

- Um externe Desktop-Geräte über eine Internetverbindung mit dem Administrationsserver zu verbinden, muss das Installationspaket für den Administrationsagenten angepasst werden. Wählen Sie in den Einstellungen des erstellen Installationspakets die Option **Erweitert → Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen** und geben Sie anschließend das neu erstelle Verbindungs-Gateway an.

Für ein Verbindungs-Gateway, das sich in der demilitarisierten Zone befindet, erstellt der Administrationsserver ein Zertifikat, das vom Zertifikat des Administrationsservers signiert ist. Wenn der Administrator die Entscheidung gefasst hat, für den Administrationsserver das Benutzerzertifikat festzulegen, muss dies bis zum Erstellen des Verbindungs-Gateways in der demilitarisierten Zone erfolgen.

Wenn es Mitarbeiter mit Laptops gibt, die sich mit dem Administrationsserver sowohl aus dem lokalen Netzwerk als auch aus dem Internet verbinden, kann es zweckmäßig sein, in der Richtlinie des Administrationsagenten eine Regel zum Umschalten des Administrationsagenten zu erstellen.

Über Verteilungspunkte

Ein Gerät, auf dem der Administrationsagent installiert ist, kann als Verteilungspunkt verwendet werden. In diesem Modus kann der Administrationsagent folgende Funktionen ausführen:

- Ausgeben von Updates, wobei Updates sowohl vom Administrationsserver als auch von den Kaspersky-Servern empfangen werden können. Im letzteren Fall muss für das Gerät, das als Verteilungspunkt dient, die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* erstellt werden:

  - Software auf anderen Geräten installieren, einschließlich Ausführung der erstmaligen Bereitstellung der Administrationsagenten auf den Geräten.

  - Das Netzwerk abfragen, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden. Der Verteilungspunkt kann dieselben Methoden zur Gerätesuche ausführen wie der Administrationsserver.

Die Bereitstellung von Verteilungspunkten in einem Unternehmensnetzwerk hat die folgenden Ziele:

- Entlastung des Administrationsservers.

- Optimieren des Datenverkehrs.

- Dem Administrationsserver wird Zugriff auf Geräte gewährt, die sich an schwer erreichbaren Standorten des Unternehmensnetzwerks befinden. Wenn sich ein Verteilungspunkts in einem Netzwerk, hinter einer NAT befindet (in Bezug auf den Administrationsserver), kann der Administrationsserver Folgendes tun:

  - Nachrichten an Geräte in IPv4- oder IPv6-Netzwerken über UDP versenden

  - Das IPv4- oder IPv6-Netzwerk abfragen

- Erstmalige Bereitstellung ausführen
- Als Push-Server fungieren

Ein Verteilungspunkt wird für eine Administrationsgruppe bestimmt. In diesem Fall umfasst der Bereich des Verteilungspunktes alle Geräte, die sich in der Administrationsgruppe und allen ihren Untergruppen befinden. Dabei muss sich das Gerät, das als Verteilungspunkt fungiert, nicht in der Administrationsgruppe befinden, welcher es zugewiesen wurde.

Sie können einen Verteilungspunkt als Verbindungs-Gateway nutzen. Die Geräte, die zum Bereich des Verteilungspunktes gehören, werden in diesem Fall nicht direkt, sondern über ein Gateway mit dem Administrationsserver verbunden. Dieser Modus kann in Szenarien nützlich sein, bei denen keine direkte Verbindung zwischen dem Administrationsserver und den verwalteten Geräten möglich ist.

Wenn Sie ein Linux-basiertes Gerät als Verteilungspunkt verwenden, wird es dringend empfohlen, die Anzahl der Datei-Deskriptoren für den klnagent-Dienst zu erhöhen. Dies ist notwendig, da der Gültigkeitsbereich des Verteilungspunkts so viele Geräte umfassen kann, dass die standardmäßige maximale Anzahl von Dateien, die geöffnet werden können, nicht ausreicht.

Anzahl der Datei-Deskriptoren für den klnagent-Dienst erhöhen

Wenn der Gültigkeitsbereich eines Linux-basierten Verteilungspunkts viele Geräte umfasst, ist die standardmäßige Beschränkung der Dateien, die geöffnet werden können (Datei-Deskriptoren), möglicherweise nicht ausreichend. Um dies zu vermeiden, können Sie das Limit der Datei-Deskriptoren für den klnagent-Dienst erhöhen.

So erhöhen Sie die Anzahl der Datei-Deskriptoren für den klnagent-Dienst:

1. Führen Sie auf dem Linux-basierten Gerät, das als Verteilungspunkt agiert, den folgenden Befehl aus:

   ```
   systemctl edit klnagent64.service
   ```

2. Geben Sie die harte und weiche Obergrenze der Dateideskriptoren im Parameter `LimitNOFILE` des Abschnitts `[Service]` an:

   `LimitNOFILE=<soft resource limit>:<hard resource limit>`

   Beispiel: `LimitNOFILE=32768:131072`. Beachten Sie, dass die flexible Beschränkung der Datei-Deskriptoren kleiner oder gleich der festen Beschränkung sein muss.

3. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Parameter korrekt angegeben wurden:

   ```
   systemd-analyze verify klnagent64.service
   ```

   Bei ungültigen Parameterangaben kann dieser Befehl einen der folgenden Fehler ausgeben:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Wenn dieser Fehler auftritt, sind in der Zeile `LimitNOFILE` falsche Zeichen angegeben. Überprüfen und korrigieren Sie die eingegebene Zeile.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Wenn dieser Fehler auftritt, liegt die flexible Beschränkung der eingegebenen Datei-Deskriptoren über der festen Beschränkung. Überprüfen Sie die eingegebene Zeile und stellen Sie sicher, dass die flexible Beschränkung der Datei-Deskriptoren kleiner oder gleich der festen Beschränkung ist.

4. Führen Sie den folgenden Befehl aus, um den Prozess "systemd" neu zu laden:

   ```
   systemctl daemon-reload
   ```

5. Führen Sie den folgenden Befehl aus, um den Dienst des Administrationsagenten neu zu starten:

   ```
   systemctl restart klnagent
   ```

6. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die angegebenen Parameter korrekt angewendet werden:

   ```
   less /proc/<Prozess-ID von nagent>/limits
   ```

   wobei `<Prozess-ID von nagent>` der Prozess-ID des Administrationsagenten entspricht. Um die Prozess-ID zu erfahren, können Sie den folgenden Befehl ausführen:

   ```
   ps -ax | grep klnagent
   ```

Die Anzahl der Dateien, die geöffnet werden können, für den Linux-basierten Verteilungspunkt wurde erhöht.

Anzahl und Konfiguration der Verteilungspunkte bestimmen

Je mehr Client-Geräte ein Netzwerk enthält, desto mehr Verteilungspunkte sind erforderlich. Es wird empfohlen, die automatische Zuweisung von Verteilungspunkten nicht zu deaktivieren. Bei aktivierter automatischer Zuweisung der Verteilungspunkte weist der Administrationsserver bei einer großen Anzahl an Client-Geräten automatisch Verteilungspunkte zu und bestimmt ihre Konfiguration.

Verwendung exklusiv zugewiesener Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte eine Reihe von bestimmten Geräten zu verwenden (d. h., exklusiv zugewiesene Server), so können Sie auf die automatische Zuweisung der Verteilungspunkte verzichten. Überzeugen Sie sich in diesem Fall davon, dass die Geräte, die Sie zu Verteilungspunkten bestimmen möchten, über ausreichend freien Speicherplatz auf dem Datenträger verfügen, nicht regelmäßig abgeschaltet werden und dass auf ihnen der Ruhezustand deaktiviert ist.

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–100	1
Über 100	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Verwendung von Standard-Client-Geräten (Workstations) als Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte Standard-Client-Geräte (d. h., Workstations) zu verwenden, wird zur Vermeidung einer unnötigen Belastung des Administrationsservers empfohlen, die Verteilungspunkte auf folgende Weise zuzuweisen (s. nachfolgende Tabelle):

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–30	1
31–300	2
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Wenn ein Verteilungspunkt abgeschaltet (oder aus anderen Gründen nicht verfügbar) ist, können die verwalteten Geräte in seinem Bereich Updates vom Administrationsserver abrufen.

Hierarchie des Administrationsservers

Beim MSP kann mehr als ein Administrationsserver vorhanden sein. Die Verwaltung mehrerer vereinzelter Administrationsserver ist unpraktisch, deshalb es ist zweckmäßig, sie in einer Hierarchie zusammenzufassen. Eine "Primär/Sekundär"-Konfiguration für zwei Administrationsserver bietet die folgenden Möglichkeiten:

- Der sekundäre Administrationsserver erbt vom primären Administrationsserver die Richtlinien und Aufgaben, wobei duplizierte Einstellungen entfernt werden.
- Die Geräteauswahlen auf dem primären Administrationsserver können Geräte der sekundären Administrationsserver einschließen.
- Die Berichte auf dem primären Administrationsserver können Daten (einschließlich ausführlicher Informationen) der sekundären Administrationsserver einschließen.

Der primäre Administrationsserver empfängt Daten von sekundären Administrationsservern, die nicht virtuell sind, nur im Rahmen der oben aufgeführten Optionen. Diese Einschränkung gilt nicht für virtuelle Administrationsserver, welche die Datenbank mit ihrem primären Administrationsserver teilen.

Virtuelle Administrationsserver

Im Rahmen des physischen Administrationsservers können mehrere virtuelle Administrationsserver erstellt werden, die in vieler Hinsicht sekundären Servern ähnlich sind. Im Vergleich zum Modell des geteilten Zugriffs, der auf den Listen der Zugriffskontrolle (ACL) beruht, ist das Modell der virtuellen Administrationsserver funktioneller und bietet eine hohe Stufe der Isolierung. Neben der eigenen Struktur der Administrationsgruppen für verwaltete Geräte mit Richtlinien und Aufgaben hat jeder virtuelle Administrationsserver auch eine eigene Gruppe von nicht zugeordneten Geräten, die über eigene Sätze von Berichten, Geräteauswahlen und Ereignissen, Installationspakete, Regeln zur Verschiebung von Geräten usw. verfügt. Die Funktionalität der virtuellen Administrationsserver kann sowohl von Dienstanbietern (xSP) zur maximalen Isolierung verschiedener Kunden voneinander, als auch von großen Unternehmen mit komplizierter Struktur und einer großen Anzahl von Administratoren verwendet werden.

Virtuelle Administrationsserver ähneln in vieler Hinsicht sekundären Administrationsservern, haben jedoch die folgenden Unterschiede:

- Einem virtuellen Administrationsserver fehlt eine Vielzahl der globalen Einstellungen und eigenen TCP-Ports
- Ein virtueller Administrationsserver hat keine sekundären Administrationsserver
- Ein virtueller Administrationsserver kann keine eigenen virtuellen Administrationsserver haben
- Auf dem physischen Administrationsserver sind die Geräte, Gruppen, Ereignisse und Objekte der verwalteten Geräte (Elemente der Quarantäne, Programm-Registry und andere) aller seiner virtuellen Administrationsserver sichtbar
- Ein virtueller Administrationsserver kann das Netzwerk nur mittels der mit ihm verbundenen Verteilungspunkte abfragen

Informationen zu Einschränkungen von Kaspersky Security Center

In der nachfolgenden Tabelle sind die Einschränkungen der aktuellen Version von Kaspersky Security Center aufgelistet.

Einschränkungen von Kaspersky Security Center

Typ der Einschränkung	Wert
Maximale Anzahl verwalteter Geräte eines Administrationsservers	100.000
Maximale Anzahl von Geräte mit aktivierter Option **Verbindung mit Administrationsserver nicht trennen**	300
Maximale Anzahl von Administrationsgruppen	10.000
Maximale Anzahl gespeicherter Ereignisse	45.000.000
Maximale Anzahl von Richtlinien	2.000
Maximale Anzahl von Aufgaben	2.000
Maximale Gesamtanzahl von Active Directory-Objekten (Organisationseinheiten (OU) und Benutzerkonten, Geräte und Sicherheitsgruppen)	1.000.000
Maximale Anzahl der Profile in der Richtlinie	100
Maximale Anzahl der sekundären Administrationsserver bei einem primären Administrationsserver	500
Maximale Anzahl der virtuellen Administrationsserver	500
Maximale Anzahl der Geräte, die ein einzelner Verteilungspunkt abdecken kann (Verteilungspunkte können nur nicht-mobile Geräte abdecken)	10.000

Typ der Einschränkung	Wert
Maximale Anzahl der Geräte, die ein einzelnes Verbindungs-Gateway verwenden können	10.000, inklusive mobile Geräte
Maximale Anzahl der mobilen Geräte, die ein einziger Administrationsserver verwalten kann	100.000, abzüglich der Anzahl der stationären verwalteten Geräte

Netzwerkbelastung

Diesem Abschnitt können Informationen über den Umfang des Datenverkehrs im Netzwerk entnommen werden, mit dem zwischen den Client-Geräten und dem Administrationsserver bei wichtigen administrativen Vorgängen Daten ausgetauscht werden.

Die Grundbelastung des Netzwerks hängt mit folgenden Szenarios zusammen:

- Erstmalige Bereitstellung des Antiviren-Schutzes
- Erstmaliges Update der Antiviren-Datenbanken
- Synchronisierung des Client-Geräts mit dem Administrationsserver
- Regelmäßiges Update der Antiviren-Datenbanken
- Verarbeitung von Ereignissen auf Client-Geräten durch Administrationsserver

Erstmalige Bereitstellung des Antiviren-Schutzes

Diesem Abschnitt können Informationen zum verbrauchten Datenvolumen bei der Installation des Administrationsagenten und Kaspersky Endpoint Security für Windows auf dem Client-Gerät entnommen werden (s. Tabelle unten).

Der Administrationsagent wird mit der erzwungenen Installation installiert, wenn der Administrationsserver die für die Installation benötigten Dateien in den gemeinsamen Ordner auf dem Client-Gerät kopiert hat. Nach der Installation empfängt der Administrationsagent über die Verbindung mit dem Administrationsserver das Programmpaket von Kaspersky Endpoint Security für Windows.

Datenverkehr

Szenario	Installation des Administrationsagenten für ein Client-Gerät	Installation von Kaspersky Endpoint Security für Windows für ein Client-Gerät (mit den aktualisierten Datenbanken)	Gemeinsame Installation des Administrationsagenten und Kaspersky Endpoint Security für Windows
Datenverkehr vom Client-Gerät zum Administrationsserver, KB	1638,4	7843,84	9707,52
Datenverkehr vom Administrationsserver zum Client-Gerät, KB	69990,4	259317,76	329318,4
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	71628,8	267161,6	339025,92

Nach der Installation der Administrationsagenten lässt sich auf den gewünschten Client-Geräten ein Gerät in der Administrationsgruppe als Verteilungspunkt einrichten. Er wird für das Verteilen der Installationspakete verwendet. In diesem Fall kann sich die bei erstmaliger Bereitstellung des Antiviren-Schutzes zu übertragende Datenmenge in Abhängigkeit davon, ob die Option IP-Multicast eingesetzt wird, ganz erheblich unterscheiden.

Wenn IP-Multicasting verwendet wird, werden die Installationspakete einmal an alle in der Administrationsgruppe eingeschalteten Geräte verschickt. So wird der gesamte Datenverkehr ungefähr um das n-fache verringert, wobei n der Anzahl der eingeschalteten Geräte in der Administrationsgruppe entspricht. Wenn IP-Multicast nicht verwendet wird, stimmt der gesamte Datenverkehr mit dem Datenverkehr beim Download der Programmpakete vom Administrationsserver überein. Als Quelle für den Download der Installationspakete dient nicht der Administrationsserver, sondern der Verteilungspunkt.

Erstmaliges Update der Antiviren-Datenbanken

Die Menge des übertragenen Datenverkehrs während der Erstaktualisierung von Antiviren-Datenbanken (beim erstmaligen Starten der Aufgabe für das Datenbanken-Update auf einem Client-Gerät) beträgt im Folgenden:

- Datenverkehr vom Client-Gerät zum Administrationsserver: 1,8 MB.
- Datenverkehr vom Administrationsserver zum Client-Gerät: 113 MB.
- Gesamter Datenverkehr (für ein Client-Gerät): 114 MB.

Die aufgeführten Daten können je nach Version der Antiviren-Datenbank etwas abweichen.

Synchronisierung des Clients mit dem Administrationsserver

Dieses Szenario charakterisiert den Zustand des Administrationssystems, in dem die Daten zwischen dem Client-Gerät und dem Administrationsserver aktiv synchronisiert werden. Die Client-Geräte stellen innerhalb der durch den Administrator vorgegebenen Fristen eine Verbindung zum Administrationsserver her. Der Administrationsserver vergleicht den Datenzustand auf dem Client-Gerät mit dem Datenzustand auf dem Server, registriert die Daten über die letzte Verbindung des Client-Geräts in der Datenbank und synchronisiert die Daten.

Diesem Abschnitt können Informationen zum Datenverkehr in die wichtigsten administrativen Szenarios bei der Verbindung des Clients mit dem Administrationsserver mit Synchronisierung entnommen werden (s. Tabelle unten). Die in der Tabelle aufgeführten Daten können je nach Version der Antiviren-Datenbank etwas abweichen.

Datenverkehr

Szenario	Datenverkehr von Client-Geräten zum Administrationsserver, KB	Datenverkehr vom Administrationsserver zu den Client-Geräten, KB	Allgemeiner Datenverkehr (für ein Client-Gerät), KB
Erstmalige Synchronisierung vor dem Datenbanken-Update auf dem Client-Gerät	699,44	568,42	1267,86
Erstmalige Synchronisierung nach dem Datenbanken-Update auf dem Client-Gerät	735,8	4474,88	5210,68
Synchronisierung bei fehlenden Änderungen auf dem Client-Gerät und auf dem Administrationsserver	11,99	6,73	18,72
Synchronisierung bei Änderung einer Einstellung in der Gruppenrichtlinie	9,79	11,39	21,18
Synchronisierung bei Änderung einer Einstellung in der Gruppenaufgabe	11,27	11,72	22,99
Erzwungene Synchronisierung bei fehlenden Änderungen auf dem Client-Gerät	77,59	99,45	177,04

Der Umfang des allgemeinen Datenverkehrs unterscheidet sich in Abhängigkeit davon, ob die Option IP-Multicast innerhalb der Administrationsgruppen eingesetzt wird, ganz erheblich. Bei Einsatz von IP-Multicast verringert sich der gesamte Datenverkehr in eine Gruppe ungefähr um das N-fache, wobei N der Anzahl der aktivierten Geräte in der Administrationsgruppe entspricht.

Der Umfang des Verkehrs bei der erstmaligen Synchronisierung vor und nach dem Datenbanken-Update wird für folgende Fälle angegeben:

- Installation des Administrationsagenten und der Sicherheitsanwendung auf dem Client-Gerät
- Verschieben des Client-Geräts in die Administrationsgruppe
- Anwendung der standardmäßig für die Gruppe erstellten Richtlinien und Aufgaben auf das Client-Gerät

In der Tabelle wird der Umfang des Datenverkehrs bei der Veränderung einer der Schutzeinstellungen angezeigt, die zu den Richtlinieneinstellungen von Kaspersky Endpoint Security gehören. Die Daten für andere Richtlinieneinstellungen können sich von den in der Tabelle dargestellten Daten unterscheiden.

Zusätzliches Update der Antiviren-Datenbanken

Die Menge an Datenverkehr bei einem inkrementellen Update der Antiviren-Datenbanken, das 20 Stunden nach dem letzten Update erfolgt, beträgt im Folgenden:

- Datenverkehr vom Client-Gerät zum Administrationsserver: 169 KB.
- Datenverkehr vom Administrationsserver zum Client-Gerät: 16 MB.
- Gesamter Datenverkehr (für ein Client-Gerät): 16,3 MB.

Die in der Tabelle aufgeführten Daten können je nach Version der Antiviren-Datenbank etwas abweichen.

Der Umfang des Datenverkehrs unterscheidet sich in Abhängigkeit davon, ob die Option IP-Multicast innerhalb der Administrationsgruppen eingesetzt wird, erheblich. Bei Einsatz von IP-Multicast verringert sich der gesamte Datenverkehr in eine Gruppe ungefähr um das N-fache, wobei N der Anzahl der aktivierten Geräte in der Administrationsgruppe entspricht.

Verarbeitung von Ereignissen der Clients durch Administrationsserver

Dieser Abschnitt enthält Informationen über das Volumen des übertragenen Datenverkehrs, wenn auf einem Client-Gerät das Ereignis "Virus gefunden" eintritt, welches an den Administrationsserver übertragen und in der Datenbank registriert wird (siehe Tabelle unten).

Datenverkehr

Szenario	Übertragen von Daten an Administrationsserver bei Auftreten des Ereignisses "Virus gefunden"	Übertragen von Daten an Administrationsserver bei Auftreten von 9 Ereignissen "Virus gefunden"
Datenverkehr vom Client-Gerät zum Administrationsserver, KB	49,66	64,05
Datenverkehr vom Administrationsserver zum Client-Gerät, KB	28,64	31,97
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	78,3	96,02

Die in der Tabelle aufgeführten Daten können in Abhängigkeit von der verwendeten Version des Antiviren-Programms und davon, welche Ereignisse in der Richtlinie in der Administrationsserver-Datenbank als erfassungswürdig definiert sind, etwas abweichen.

Datenverkehr in 24 Stunden

Diesem Abschnitt können Informationen zum verbrauchten Datenvolumen für 24 Stunden entnommen werden, in den sich das Administrationssystem im Ruhezustand befindet, wenn keine Änderungen von der Seite der Client-Geräte oder des Administrationsservers vorgenommen wurden (s. Tabelle unten).

Die in der Tabelle aufgeführten Daten erläutern den Netzwerkstatus nach der Standardinstallation von Kaspersky Security Center und Fertigstellung des Schnellstartassistenten. Das Synchronisierungsintervall des Client-Geräts mit dem Administrationsserver betrug 20 Minuten, der Update-Download in die Datenverwaltung des Administrationsservers erfolgte stündlich.

Raten für den Datenverkehr pro 24 Stunden im Ruhezustand

Datenfluss	Wert
Datenverkehr vom Client-Gerät zum Administrationsserver, KB	3235,84
Datenverkehr vom Administrationsserver zum Client-Gerät, KB	64,378.88
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	67,614.72

Vorbereitung auf die Verwaltung mobiler Geräte

Dieser Abschnitt enthält Informationen:

- Über den iOS MDM-Server zur Verwaltung der iOS-Geräte mittels darauf installierten speziellen iOS MDM-Profilen
- Über die Verwaltung von mobilen Geräte mit installiertem Kaspersky Endpoint Security für Android

iOS MDM-Server

Der iOS MDM-Server erlaubt die Verwaltung der iOS-Geräte mittels darauf installierten speziellen iOS MDM-Profilen. Es werden folgende Funktionen unterstützt:

- Sperrung des Geräts
- Zurücksetzen des Kennworts
- Datenlöschung auf dem Gerät
- Installation bzw. Deinstallation von Apps
- Anwendung des iOS MDM-Profils mit erweiterten Einstellungen (wie die Einstellungen für VPN, E-Mail, WLAN, Kamera, Zertifikate und so weiter)

Der iOS MDM-Server ist ein Webdienst, der eingehende Verbindungen von mobilen Geräten auf dem TLS-Port (standardmäßig Port 443) übernimmt und seitens Kaspersky Security Center mithilfe des Administrationsagenten verwaltet wird. Der Administrationsagent wird lokal auf dem Gerät mit verteiltem iOS MDM-Server installiert.

Während der Bereitstellung des iOS MDM-Servers muss der Administrator wie folgt vorgehen:

- Dem Administrationsagenten den Zugriff auf den Administrationsserver gewährleisten
- Den mobilen Geräten den Zugriff auf den TCP-Port des iOS MDM-Servers gewährleisten

In diesem Abschnitt werden zwei typische Konfigurationen des iOS MDM-Servers betrachtet.

Typische Konfiguration: Kaspersky Device Management für iOS in der DMZ

Der iOS MDM-Server befindet sich in der demilitarisierten Zone des Unternehmensnetzwerks mit Internetzugang. Eine Besonderheit dieser Vorgehensweise ist das Vermeiden von Problemen, wenn Geräte über das Internet auf den iOS MDM-Webdienst zugreifen.

Da für die Verwaltung des iOS MDM-Servers ein lokal installierter Administrationsagent erforderlich ist, muss die Interaktion dieses Administrationsagenten mit dem Administrationsserver gewährleistet sein. Dies können Sie auf eine der folgenden Arten gewährleisten:

- Durch das Verschieben des Administrationsservers in die DMZ.
- Durch die Verwendung eines Verbindungs-Gateways:
  a. Verbinden Sie den auf dem Gerät mit bereitgestelltem iOS MDM-Server befindlichen Administrationsagenten über ein Verbindungs-Gateway mit dem Administrationsserver.
  b. Bestimmen Sie den auf dem Gerät mit bereitgestelltem iOS MDM-Server befindlichen Administrationsagenten zum Verbindungs-Gateway.

Typische Konfiguration: iOS MDM-Server im lokalen Netzwerk des Unternehmens

Der iOS MDM-Server befindet sich innerhalb des Unternehmensnetzwerks. Der Port 443 (Standardport) muss für den externen Zugriff aktiviert sein. Dies kann beispielsweise durch Veröffentlichung des iOS MDM-Webdienstes auf einem Reverse-Proxy geschehen, der die erzwungene Delegierung von Kerberos unterstützt.

In einer beliebigen typischen Konfiguration muss die Verfügbarkeit der Apple-Webdienste (Adressbereich 17.0.0.0/8) über Port TCP 2197 für die iOS MDM-Server gewährleistet sein. Dieser Port wird dazu verwendet, die Geräte über den speziellen Dienst APNs von neuen Befehlen zu benachrichtigen.

Mobile Geräte mit installiertem Kaspersky Endpoint Security für Android verwalten

Die Verwaltung von mobilen Geräten mit installierter App Kaspersky Endpoint Security für Android™ (im Weiteren KES-Geräte) erfolgt mithilfe des Administrationsservers. Kaspersky Security Center unterstützt die folgenden Funktionen zur Verwaltung von KES-Geräten:

- Arbeit mit mobilen Geräten und den Client-Geräten:
  - Zugehörigkeit zu Administrationsgruppen
  - Überwachung, z. B. Anzeigen von Statuswerten, Ereignissen und Berichten
  - Änderung der lokalen Einstellungen und Festlegung der Richtlinie für die App Kaspersky Endpoint Security für Android
- Zentralisierter Versand von Befehlen
- Remote-Installation der Pakete mit mobilen Anwendungen

Der Administrationsserver verwaltet KES-Geräte über TLS, TCP-Port 13292.

Informationen zur Leistungsfähigkeit des Administrationsservers

In diesem Abschnitt sind die Ergebnisse der Leistungstests des Administrationsservers für verschiedene Hardwarekonfigurationen sowie die Einschränkungen für die Verbindung verwalteter Geräte mit dem Administrationsserver aufgeführt.

Einschränkungen der Verbindung mit dem Administrationsserver

Der Administrationsserver unterstützt die Verwaltung von bis zu 100.000 Geräten ohne Verlust der Leistung.

Beschränkungen von Verbindungen mit dem Administrationsserver ohne Verlust der Leistung:

- Ein Administrationsserver kann bis zu 500 virtuelle Administrationsserver unterstützen.
- Der primäre Administrationsserver unterstützt maximal 1.000 Sitzungen gleichzeitig.
- Die virtuellen Administrationsserver unterstützen nicht mehr als 1.000 Sitzungen gleichzeitig.

Ergebnisse der Leistungstests des Administrationsservers

Mit den Testdaten für die Leistungsfähigkeit des Administrationsservers wurde die maximale Anzahl an Client-Geräten definiert, mit denen der Administrationsserver eine Synchronisierung in den vorgegebenen Zeiträumen ausführen kann. Sie können diese Informationen dazu nutzen, das optimale Schemata für die Bereitstellung des Antiviren-Schutzes in Computernetzwerken zu wählen.

Zu Testzwecken wurden Geräte mit den folgenden Hardwarekonfigurationen verwendet (s. Tabellen unten):

Hardwarekonfiguration des Administrationsservers

Parameter	Wert
Prozessor	Intel Xeon CPU E5630, Taktfrequenz 2,53 GHz, 2 Socket, 8 Kerne, 16 logische Prozessoren
Arbeitsspeicher	26 GB
Festplatte	IBM ServeRAID M5014 SCSI Disk Device, 487 GB
Betriebssystem	Microsoft Windows Server 2019 Standard, Version 10.0.17763, Build 17763
Netzwerk	QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client)

Hardwarekonfiguration des Geräts mit SQL Server

Parameter	Wert
Prozessor	Intel Xeon CPU X5570, Taktfrequenz 2,93 GHz, 2 Sockets, 8 Kerne, 16 logische Prozessoren
Arbeitsspeicher	32 GB
Festplatte	Adaptec Array SCSI Disk Device, 2047 GB
Betriebssystem	Microsoft Windows Server 2019 Standard, Version 10.0.17763, Build 17763
Netzwerk	Intel 82576 Gigabit

Der Administrationsserver unterstützte das Erstellen von 500 virtuellen Administrationsservern.

Der Synchronisierungszeitraum betrug 15 Minuten für je 10.000 verwaltete Geräte (s. Tabelle unten).

Ergebnisse der zusammengefassten Belastungstests des Administrationsservers

Synchronisierungsintervall (Min.)	Anzahl der verwalteten Geräte
15	10.000
30	20.000

Synchronisierungsintervall (Min.)	Anzahl der verwalteten Geräte
45	30.000
60	40.000
75	50.000
90	60.000
105	70.000
120	80.000
135	90.000
150	100.000

Falls Sie den Administrationsserver mit einem MySQL-, oder SQL Express-Datenbankserver verbinden, wird nicht empfohlen, das Programm zur Verwaltung von mehr als 10.000 Geräten zu verwenden. Für das MariaDB-DBMS beträgt die empfohlene maximale Anzahl verwalteter Geräte 20.000 Stück.

Ergebnisse der Leistungstests des KSN-Proxyservers

Wenn Ihr Unternehmensnetzwerk eine große Anzahl an Client-Geräten umfasst, die den Administrationsserver als KSN-Proxyserver verwenden, muss die Hardware des Administrationsservers bestimmte Voraussetzungen erfüllen, um die Anfragen der Client-Geräte verarbeiten zu können. Sie können die nachfolgenden Testergebnisse verwenden, um die Belastung des Administrationsservers in Ihrem Netzwerk einzuschätzen und die Hardware-Ressourcen so zu planen, dass der ordnungsgemäße Betrieb des KSN-Proxy-Service gewährleistet ist.

Die unterstehenden Tabellen zeigen die Hardwarekonfiguration für den Administrationsservers und für SQL Server auf. Diese Konfiguration wurde zum Testen verwendet.

Hardwarekonfiguration des Administrationsservers

Parameter	Wert
Prozessor	Intel Xeon CPU E5450, Taktfrequenz 3,00 GHz, 2 Socket, 8 Kerne, 16 logische Prozessoren
Arbeitsspeicher	32 GB
Betriebssystem	Microsoft Windows Server 2016 Standard

Hardwarekonfiguration für SQL Server

Parameter	Wert
Prozessor	Intel Xeon CPU E5450, Taktfrequenz 3,00 GHz, 2 Socket, 8 Kerne, 16 logische Prozessoren
Arbeitsspeicher	32 GB
Betriebssystem	Microsoft Windows Server 2019 Standard

Die nachfolgende Tabelle enthält die Testergebnisse.

Zusammenfassung der Ergebnisse der Leistungstests des KSN-Proxyservers

Parameter	Wert
Maximale Anzahl der pro Sekunde verarbeiteten Anfragen	4914
Maximale CPU-Auslastung	36%

Netzwerkeinstellungen zur Interaktion mit externen Diensten

Kaspersky Security Center verwendet die folgenden Netzwerkeinstellungen zur Interaktion mit externen Diensten.

Netzwerkeinstellungen

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 443 Protokoll: HTTPS	activation-v2.kaspersky.com	Aktivieren des Programms
Port: 443 Protokoll: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky
Port: 443 Protokoll: HTTPS	https://downloads.upd.kaspersky.com	• Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky • Es wird geprüft, ob auf die Kaspersky-Server zugegriffen werden kann. Vor dem Herunterladen von Kaspersky-Datenbanken und Softwaremodulen überprüft Kaspersky Security Center, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server.

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 80 Protokoll: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky
Port: 443 Protokoll: HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Verwenden von Kaspersky Security Network
Port: 443, 1443 Protokoll: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Verwenden von Kaspersky Security Network
Port: 443 Protokoll: HTTPS	click.kaspersky.com redirect.kaspersky.com	Folgen von Links aus der Benutzeroberfläche

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 80 Protokoll: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Diese Server sind Teil der Public Key Infrastructure (PKI) und werden benötigt, um die Gültigkeit der Zertifikate mit den digitalen Signaturen von Kaspersky zu überprüfen. Die CRL ist eine Liste mit Zertifikaten, die widerrufen wurden. Mittels OCSP können Sie den Status eines bestimmten Zertifikats in Echtzeit abfragen. Diese Server erhöhen die Sicherheit bei der Interaktion mit digitalen Zertifikaten und schützen vor möglichen Angriffen.
Port: 443 Protokoll: HTTPS	https://ipm-klca.kaspersky.com	Marketing-Mitteilungen

Berücksichtigen Sie die folgenden Empfehlungen, damit Kaspersky Security Center ordnungsgemäß mit externen Diensten interagiert:
- Auf den Netzwerkgeräten und dem Proxyserver Ihres Unternehmens muss auf den Ports 443 und 1443 unverschlüsselter Netzwerkdatenverkehr erlaubt sein.
- Wenn der Administrationsserver mit den Kaspersky-Update-Servern und den Servern von Kaspersky Security Network interagiert, muss verhindert werden, dass der Netzwerkdatenverkehr durch das Ersetzen von Zertifikaten übernommen wird (MITM-Angriffe).

So laden Sie mit dem Tool "klscflag" Updates über das HTTP- oder HTTPS-Protokoll herunter:

1. Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

2. Wenn Sie Updates über das HTTP-Protokoll herunterladen möchten, führen Sie einen der folgenden Befehle aus:

   - Auf dem Gerät mit installiertem Administrationsserver:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Auf einem Verteilungspunkt:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Wenn Sie Updates über das HTTPS-Protokoll herunterladen möchten, führen Sie einen der folgenden Befehle aus:

   - Auf dem Gerät mit installiertem Administrationsserver:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Auf einem Verteilungspunkt:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Softwareverteilung für den Administrationsagenten und die Sicherheitsanwendung

Zur Verwaltung der Unternehmensgeräte muss auf den Geräten der Administrationsagent installiert werden. Die Bereitstellung der verteilten App Kaspersky Security Center auf den Geräten des Unternehmens beginnt gewöhnlich mit der Installation des Administrationsagenten.

Unter Windows XP führt der Administrationsagent folgende Operationen möglicherweise nicht korrekt aus: Das Herunterladen von Updates direkt von den Servern von Kaspersky (als Verteilungspunkt), das Fungieren als KSN-Proxyserver (als Verteilungspunkt) und das Erkennen von Schwachstellen bei Drittanbietern (wenn die Funktion Schwachstellen- und Patch-Management genutzt wird).

Erstmalige Bereitstellung

Zur Verwaltung der Unternehmensgeräte muss auf jedem Gerät der Administrationsagent installiert werden.

Die Installation des Administrationsagenten auf einem verwalteten Windows-Gerät kann wie folgt erfolgen:

- Mithilfe von Drittanbieter-Tools zur Remote-Installation von Apps.
- Durch Klonen eines Festplatten-Image mit dem Betriebssystem und dem installierten Administrationsagenten, durch von Kaspersky Security Center für die Arbeit mit Laufwerks-Images bereitgestellten Tools, oder durch Drittanbieter-Tools.
- Über den Mechanismus der Microsoft Windows-Gruppenrichtlinien durch die Standardtools zur Verwaltung von Microsoft Windows-Gruppenrichtlinien oder automatisiert durch die entsprechende Option in der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center.
- Im erzwungenen Modus, indem die Betriebssystem-Ressourcen durch die Aufgabe zur Remote-Installation von Kaspersky Security Center verwendet werden.
- Mittels Versand eines Links auf die von Kaspersky Security Center gebildeten autonomen Pakete an die Benutzer der Geräte. Die autonomen Pakete stellen ausführbare Module dar, in denen die Programmpakete der ausgewählten Programme mit den konfigurierten Einstellungen enthalten sind.
- Manuell durch Starten der Installer der Programme auf den Geräten.

Die Erstinstallation des Administrationsagenten auf einem verwalteten Linux-Gerät kann wie folgt erfolgen:

- Mittels SSH-Verbindung zum verwalteten Gerät und der Ausführung der Aufgabe zur Remote-Installation.
- Durch Ausführen der Paketinstallation auf dem verwalteten Gerät.

Die Erstinstallation des Administrationsagenten auf einem verwalteten macOS-Gerät kann wie folgt erfolgen:

- Durch Ausführen der Aufgabe zur Remote-Installation über einen macOS-basierten Verteilungspunkt.
- Mittels Versand eines Links auf die von Kaspersky Security Center gebildeten autonomen Pakete an die Benutzer der Geräte. Autonomen Pakete sind ausführbare Module, in denen die Programmpakete der ausgewählten Programme mit den vorkonfigurierten Einstellungen enthalten sind.

Nachdem der Administrationsagent auf einem Gerät installiert wurde, können Sie auf diesem Gerät mittels Administrationsagent die Remote-Installation von Kaspersky-Anwendungen durchführen. Dabei wird die Übertragung des Programmpakets der zu installierenden App zusammen mit den vom Administrator festgelegten Installationseinstellungen über die Verbindungskanäle zwischen den Administrationsagenten und dem Administrationsserver durchgeführt. Für die Übertragung des Programmpakets können Sie Knoten zur weiteren Verteilung in Form von Verteilungspunkten, Multicast-Versand usw. verwendet werden.

Bei der Auswahl von Methode und Strategie zur Bereitstellung der Programme im verwalteten Netzwerk muss eine Reihe von Faktoren beachtet werden (unvollständige Liste):

- Konfiguration des Unternehmensnetzwerks.
- Gesamtzahl der Geräte.
- Im Unternehmensnetzwerk vorhandene Geräte, die nicht Mitglieder der Active Directory-Domänen sind, und vorhandene einheitliche Benutzerkonten mit Administratorrechten auf solchen Geräten.
- Breite des Kanals zwischen dem Administrationsserver und den Geräten.
- Art der Verbindung zwischen dem Administrationsserver und den Remote-Subnetzen sowie die Kapazität der Netzwerkkanäle innerhalb dieser Subnetze.
- Sicherheitseinstellungen, die zu Beginn der Bereitstellung auf Remote-Geräten angewendet wurden. Mit diesen Parametern kann eine Remote-Verbindung zu dem verwalteten Gerät hergestellt und der Installer gestartet werden.

Anpassen der Einstellungen der Installer

Vor Beginn der Bereitstellung der Kaspersky-Anwendungen im Netzwerk müssen die Installationseinstellungen festgelegt werden – jene Einstellungen bestimmen, die im Verlauf der Programminstallation angepasst werden. Bei der Installation des Administrationsagenten muss zumindest die Adresse für die Verbindung mit dem Administrationsserver und, wenn möglich, auch einige erweiterte Einstellungen festgelegt werden. Abhängig von der ausgewählten Installationsmethode können die Einstellungen auf verschiedenen Weisen festgelegt werden. Jedenfalls können die erforderlichen Einstellungen (bei der interaktiven Installation manuell auf dem ausgewählten Gerät) mithilfe der Benutzerschnittstelle des Installers festgelegt werden.

Diese Methode zur Konfiguration der Einstellungen eignet sich nicht für die Silent-Installation der Programme auf den Gruppen der Geräte. Im typischen Fall muss der Administrator die Einstellungswerte, die in Folge für die Silent-Installation auf den ausgewählten Geräten im Netzwerk verwendet werden können, zentralisiert angeben.

Installationspakete

Die erste und wichtigste Methode zur Konfiguration der Installationseinstellungen der Apps ist universell und kommt für alle Installationsmethoden der Apps in Frage: sowohl mithilfe von Kaspersky Security Center als auch mithilfe der meisten Drittanbieter-Tools. Diese Methode bedingt das Erstellen der Installationspakete der Apps in Kaspersky Security Center.

Die Installationspakete werden auf folgende Arten erstellt:

- Automatisch aus den angegebenen Programmpaketen auf der Grundlage *Beschreibungen* in ihren Bestand (Dateien mit der Erweiterung kud, die Regeln für Installation und Analyse des Ergebnisses und andere Informationen enthalten)

- Aus den ausführbaren Dateien von Installern oder aus Installern im nativen Format (.msi, .deb, .rpm) für Standard- oder unterstützte Programme

Die erstellten Installationspakete bestehen aus einer Hierarchie von Ordnern mit Unterordnern und Dateien. Neben den originalen Programmpaketen umfasst das Installationspaket die bearbeiteten Einstellungen (einschließlich der Einstellungen des Installers und der Regel zur Verarbeitung von Situationen wie ein erforderlicher für den Abschluss der Installation Neustart des Betriebssystems), sowie kleine Hilfsmodule.

Die Werte der Installationseinstellungen, die spezifisch für die konkrete unterstützte App sind, können in der Benutzerschnittstelle der Verwaltungskonsole beim Erstellen des Installationspakets festgelegt werden. Im Fall einer Remote-Installation der Apps mithilfe von Kaspersky Security Center werden die Installationspakete so an die Geräte so geliefert, dass beim Start des Installers der App alle vom Administrator festgelegten Einstellungen verfügbar sind. Bei Verwendung von Drittanbieter-Tools zur Installation von Kaspersky-Anwendungen müssen Sie nur sicherstellen, dass auf dem Gerät das komplette Installationspaket verfügbar ist, also das Programmpaket und dessen Einstellungen. Die Installationspakete werden erstellt und von Kaspersky Security Center im entsprechenden Unterordner des freigegebenen Ordners aufbewahrt.

Geben Sie in den Einstellungen der Installationspakete keine Daten von privilegierten Benutzerkonten an.

Anweisungen zur Verwendung dieser Konfigurationsmethode für Kaspersky-Anwendungen vor der Bereitstellung durch Drittanbieter-Tools finden Sie im Abschnitt Bereitstellung mithilfe des Mechanismus der Gruppenrichtlinien von Microsoft Windows.

Sofort nach der Installation von Kaspersky Security Center werden automatisch mehrere Installationspakete erstellt, die bereit zur Installation sind, darunter die Pakete des Administrationsagenten und der Sicherheitsanwendungen für die Plattform Microsoft Windows.

Obwohl es möglich ist, den Lizenzschlüssel für das Programm in den Eigenschaften des Installationspakets anzugeben, sollte diese Methode der Lizenzverteilung nicht verwendet werden, da es in diesem Fall einfach ist, Lesezugriff auf Installationspakete zu erlangen. Es wird empfohlen, automatisch verteilte Lizenzschlüssel oder Aufgaben zur Installation von Lizenzschlüsseln zu verwenden.

Eigenschaften des MSI-Installers und der Transformationsdateien

Die Anpassung der Installationseinstellungen auf der Windows-Plattform ist Aufgabe der MSI-Eigenschaften und der Transformationsdateien. Diese Methode kann in folgenden Fällen verwendet werden:

- Bei der Installation mittels Windows-Gruppenrichtlinien mithilfe der Standard-Tools von Microsoft oder anderer Drittanbieter-Tools für die Arbeit mit den Windows-Gruppenrichtlinien.

- Bei der Installation mithilfe von Drittanbieter-Tools, die auf die Arbeit mit Installern im Format Microsoft Installer ausgelegt sind.

Bereitstellung mithilfe von Drittanbieter-Tools zur Remote-Installation von Apps

Sollten im Unternehmen irgendwelche Tools zur Remote-Installation von Apps vorhanden sein (beispielsweise Microsoft System Center), ist es sinnvoll, die erstmalige Bereitstellung mithilfe dieser Tools auszuführen.

Folgende Aktionen müssen ausgeführt werden:

- Die Konfigurationsart für die Installationseinstellungen auswählen, die sich am besten für die verwendete Methode der Bereitstellung eignet.
- Den Synchronisierungsmechanismus zwischen der Änderung der Einstellungen der Installationspakete über die Benutzeroberfläche der Verwaltungskonsole und der Arbeit der ausgewählten Dritthersteller-Tools zur Bereitstellung der Apps aus den betreffenden Installationspaketen bestimmen.
- Sich im Fall einer Installation aus dem freigegebenen Ordner von der ausreichenden Leistung dieser Dateiressource überzeugen.

Über Aufgaben zur Remote-Installation in Kaspersky Security Center

Kaspersky Security Center bietet eine Vielzahl von Mechanismen zur Remote-Installation von Apps, die in Form von Aufgaben zur Remote-Installation der Apps realisiert werden (erzwungene Installation, Installation mithilfe des Kopierens Festplatten-Images, Installation mithilfe der Microsoft Windows-Gruppenrichtlinien). Die Aufgabe zur Remote-Installation kann sowohl für die angegebene Administrationsgruppe als auch für eine Reihe von Geräten oder für Geräteauswahlen erstellt werden (diese Aufgaben werden in der Verwaltungskonsole im Ordner **Aufgaben** angezeigt). Beim Erstellen der Aufgabe können die Installationspakete (des Administrationsagenten und/oder anderer Anwendungen) ausgewählt werden, die mithilfe der betreffenden Aufgabe installiert werden, sowie eine Reihe von Einstellungen festgelegt werden, mit denen die Art der Remote-Installation bestimmt wird. Darüber hinaus kann der Assistent für Remote-Installationen von Apps verwendet werden, dem das Erstellen der Aufgabe zur Remote-Installation von Apps und das Monitoring der Ergebnisse zugrunde liegt.

Aufgaben für Administrationsgruppen gelten nicht nur auf den Geräten, die zu dieser Gruppe gehören, sondern auch auf allen Geräte aller Untergruppen der ausgewählten Gruppe. Wenn in den Aufgabeneinstellungen die entsprechende Einstellung aktiviert ist, erstreckt sich die Aufgabe auf die Geräte der sekundären Administrationsserver, die sich in der betreffenden Gruppe oder ihren Untergruppen befinden.

Aufgaben für eine Reihe von Geräten aktualisieren die Liste der Client-Geräte bei jedem Start entsprechend der Zusammensetzung der Geräteauswahlen zum Zeitpunkt des Aufgabenstarts. Wenn sich in der Geräteauswahl Geräte befinden, die mit sekundären Administrationsservern verbunden sind, wird die Aufgabe auch auf diesen Geräten ausgeführt. Details über diese Einstellungen und die Installationsmethoden werden in diesem Abschnitt beschrieben.

Für die erfolgreiche Ausführung der Aufgabe zur Remote-Installation auf Geräten, die mit sekundären Administrationsserver verbunden sind, müssen die von der Aufgabe verwendeten Installationspakete vorher mithilfe der Aufgabe zur Relaisübertragung an die entsprechenden sekundären Administrationsserver weitergeleitet werden.

Bereitstellung durch Erstellung und Verteilung eines Geräte-Images

Wenn der Administrationsagent auf den Geräten installiert werden muss, auf denen auch das Betriebssystem und die übrige Software installiert (bzw. neu installiert) werden sollen, ist es möglich, den Mechanismus zum Erstellen und Kopieren eines Geräte-Images zu verwenden.

Um die Bereitstellung durch das Erstellen und Kopieren einer Festplatte auszuführen:

1. Erstellen Sie ein Referenzgerät mit einem Betriebssystem und installieren Sie darauf die erforderliche Software, einschließlich Administrationsagent und Sicherheitsanwendung.

2. Ein Image des "Mustergeräts" aufzeichnen und dieses Image anschließend mittels einer Aufgabe von Kaspersky Security Center auf die neuen Geräte verteilen.

   Für das Aufzeichnen und die Installation der Laufwerk-Images können sowohl im Unternehmen vorhandene Tools von Drittherstellern als auch die von Kaspersky Security Center bereitgestellte Funktionalität (Lizenz für Schwachstellen- und Patch-Management vorausgesetzt) verwendet werden.

Wenn für die Arbeit mit den Laufwerk-Images Tools von Drittherstellern verwendet werden, muss bei der Bereitstellung auf das Gerät aus dem Muster-Image das Löschen von Informationen gewährleistet sein, mit deren Hilfe Kaspersky Security Center das verwaltete Gerät identifiziert. Andernfalls kann der Administrationsserver die Geräte, die durch das Kopieren von ein und demselben Image erstellt wurden, im Folgenden nicht korrekt unterscheiden.

Beim Aufzeichnen des Laufwerk-Images mithilfe von Kaspersky Security Center wird dieses Problem automatisch behoben.

Kopieren des Festplatten-Images mittels Tools von Drittherstellern

Bei Verwendung von Tools von Drittherstellern für das Aufzeichnen des Images des Geräts mit dem installierten Administrationsagenten muss eine der folgenden Methoden verwendet werden:

- Empfohlene Methode. Wenn Sie den Administrationsagenten auf einem Referenzgerät installieren, erstellen Sie das Geräte-Abbild vor dem ersten Start des Administrationsagenten-Dienstes (da eindeutige Informationen, mit denen das Gerät identifiziert wird, bei der ersten Verbindung des Administrationsagenten mit dem Administrationsserver erstellt werden). Im Folgenden ist es empfehlenswert, den Start des Dienstes des Administrationsagenten bis zum Ausführen der Operation zum Aufzeichnen des Images nicht zuzulassen.

- Auf dem geeichten Gerät, den Dienst des Administrationsagenten anhalten und das Tool klmover mit dem Parameter -dupfix ausführen. Das Tool klmover ist Teil des Installationspakets des Administrationsagenten. Vermeiden Sie die erneute Ausführung des Administrationsagenten, bis der Vorgang zum Aufzeichnen des Images abgeschlossen ist.

- Nach dem Bereitstellen des Images ist es beim ersten Start des Betriebssystems erforderlich, dass klmover mit dem "-dupfix"-Parameter vor dem ersten Start des Administrationsagenten auf den Zielgeräten ausgeführt wird. Das Tool "klmover" ist Teil des Installationspakets des Administrationsagenten.

- Verwenden Sie den "Laufwerk klonen"-Modus des Administrationsagenten.

Wenn das Festplatten-Image fehlerhaft kopiert wurde, können Sie das Problem beheben.

Sie können auch ein Image von einem Gerät erstellen, auf dem der Administrationsagent nicht installiert ist. Verteilen Sie dazu die Images auf den Zielgeräten und stellen Sie anschließend den Administrationsagenten bereit. Wenn Sie diese Methode verwenden, müssen Sie den Zugriff auf den Netzwerkordner mit autonomen Installationspaketen von einem Gerät aus gewähren.

Fehlerhaftes Kopieren eines Festplatten-Images

Wenn ein Image-Festplatte mit installiertem Administrationsagenten kopiert wurde, ohne die Bereitstellungsregeln zu beachten, können einige Geräte in der Verwaltungskonsole gemeinsam unter einem einzigen Symbol mit einem sich ständig ändernden Namen angezeigt werden.

Sie können das Problem auf eine der folgenden Arten beheben:

- Administrationsagent entfernen

  Diese Methode ist am zuverlässigsten. Auf Geräten aus einer fehlerhaften Image-Kopie müssen Sie den Administrationsagenten mithilfe von Drittanbieter-Tools entfernen und ihn anschließend erneut installieren. Der Administrationsagent kann nicht über die Tools von Kaspersky Security Center entfernt werden, da der Administrationsserver nicht zwischen fehlerhaften Geräten unterscheiden kann (alle haben dasselbe Symbol in der Verwaltungskonsole).

- Ausführen des Tools "klmover" mit dem Parameter "-dupfix"

  Verwenden Sie Tools von Drittanbietern, um das Tool "klmover" mit dem Parameter "-dupfix" ("klmover -dupfix") einmal auf fehlerhaften Geräten (die aus einer fehlerhaften Image-Kopie stammen) auszuführen. Das Tool "klmover" befindet sich im Installationsordner des Administrationsagenten. Sie können das Tool nicht mit den Werkzeugen von Kaspersky Security Center ausführen, da der Administrationsserver nicht zwischen fehlerhaften Geräten unterscheiden kann (alle haben dasselbe Symbol in der Verwaltungskonsole).

  Löschen Sie anschließend das Symbol, auf dem die fehlerhaften Geräte angezeigt wurden, bevor Sie das Tool ausführen.

- Regelverschärfung zur Erkennung falsch kopierter Geräte.

  Diese Methode ist nur verwendet werden, wenn der Administrationsserver und die Administrationsagenten in Version 10 Service Pack 1 oder höher installiert sind.

  Die Regel zur Erkennung fehlerhaft kopierter Administrationsagenten muss verschärft werden, damit die Änderung des NetBIOS-Namens eines Geräts automatisch zu einer "Korrektur" dieser Administrationsagenten führt (unter der Annahme, dass alle kopierten Geräte eindeutige NetBIOS-Namen haben).

Auf dem Gerät mit dem Administrationsserver müssen Sie die unten angezeigte reg-Datei in die Registrierung importieren und anschließend den Dienst des Administrationsservers neu starten.

- Wenn auf dem Gerät mit dem Administrationsserver ein 32-Bit-Betriebssystem läuft:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

- Wenn auf dem Gerät mit dem Administrationsserver ein 64-Bit-Betriebssystem läuft:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Bereitstellung mithilfe des Mechanismus der Gruppenrichtlinien von Microsoft Windows

Es wird empfohlen, die erstmalige Bereitstellung der Administrationsagenten bei Erfüllung der folgenden Bedingungen mithilfe der Gruppenrichtlinien von Microsoft Windows zu verwirklichen:

- Das Gerät gehört zur Domäne Active Directory.
- Der Plan zur Bereitstellung erlaubt, den standardmäßigen Neustart der Geräte abzuwarten, bevor darauf mit der Bereitstellung des Administrationsagenten begonnen wird, oder auf den Geräten kann zwangsläufig die Windows-Gruppenrichtlinie verwendet werden.

Die vorliegende Methode der Bereitstellung besteht im Wesentlichen aus Folgendem:

- Das Programmpaket im Format Microsoft Installer (MSI-Paket) wird in den freigegebenen Ordner (Ordner, für den die Benutzerkonten "LocalSystem" der Geräte Lesezugriff haben) verschoben.
- In der Gruppenrichtlinie Active Directory wird das Installationsobjekt des vorliegenden Programmpakets erstellt.
- Der Gültigkeitsbereich der Installation wird durch Anbinden an die Organisationseinheit (OU) und/oder an die Sicherheitsgruppe, zu der die Geräte gehören, angegeben.
- Bei der nächsten Anmeldung des Geräts in der Domäne (vor der Anmeldung der Benutzer des Geräts) wird geprüft, ob die erforderliche App unter den installierten Apps vorhanden ist. Wenn die App fehlt erfolgt ein Download des Programmpakets von der in der Richtlinie festgelegten Ressource und dessen Installation.

Einer der Vorteile dieser Methode der Bereitstellung ist, dass die festgelegten Apps beim Download des Betriebssystems noch vor der Anmeldung des Benutzers im System auf den Geräten installiert werden. Selbst wenn der Benutzer, der über die erforderlichen Berechtigungen verfügt, die Apps löscht, wird sie beim nächsten Download des Betriebssystems wieder installiert. Ein Nachteil dieser Methode der Bereitstellung besteht darin, dass die vom Administrator erzeugten Änderungen in der Gruppenrichtlinie bis zum Neustart der Geräte (ohne Anwendung zusätzlicher Tools) nicht in Kraft treten.

Mithilfe der Gruppenrichtlinien können sowohl der Administrationsagent als auch andere Apps installiert werden, deren Installer das Format Windows Installer haben.

Bei der Auswahl dieser Methode der Bereitstellung muss unter anderem die Belastung der Dateiressource berücksichtigt werden, von der das Kopieren der Dateien auf die Geräte bei der Anwendung der Windows-Gruppenrichtlinie ausgeführt wird.

Die Arbeit mit den Microsoft Windows-Richtlinien mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center

Am einfachsten werden Apps mithilfe der Microsoft Windows-Gruppenrichtlinien durch Aktivieren der Option **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen** in den Eigenschaften der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center installiert. In diesem Fall werden beim Start der Aufgabe des Administrationsservers folgende Aktionen selbständig ausgeführt:

- Die erforderlichen Objekte werden in der Microsoft Windows-Gruppenrichtlinie erstellt.
- Es werden spezielle Sicherheitsgruppen erstellt, in der die Geräte aktiviert werden, und die Installation der ausgewählten Apps wird diesen Sicherheitsgruppen zugewiesen. Die Zusammensetzung der Sicherheitsgruppen wird bei jedem Aufgabenstart entsprechend der Geräteauswahl zum Zeitpunkt des Starts aktualisiert.

Zur Gewährleistung der Funktionsfähigkeit der vorliegenden Funktion ist es erforderlich, in den Aufgabeneinstellungen das Benutzerkonto anzugeben, das über die Berechtigungen zum Bearbeiten Gruppenrichtlinien Active Directory verfügt.

Wenn mithilfe einer Aufgabe sowohl der Administrationsagenten als auch eine andere App installiert werden soll, führt die Aktivierung der Option **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen** dazu, dass in der Richtlinie Active Directory nur ein Installationsobjekt für den Administrationsagenten erstellt wird. Die zweite in der Aufgabe ausgewählte App wird bereits mithilfe des Administrationsagenten installiert, sobald dieser auf dem Gerät installiert ist. Wenn es aus einem bestimmten Grund erforderlich ist, eine andere App als den Administrationsagenten mithilfe der Windows-Gruppenrichtlinien zu installieren, muss die Installationsaufgabe nur für dieses Installationspaket (ohne Paket des Administrationsagenten) erstellt werden. Nicht alle Apps können mithilfe der Gruppenrichtlinien von Microsoft Windows installiert werden. Ob eine solche Möglichkeit besteht, erfahren Sie in den Informationen über die Installationsmethoden der App.

Sollten die erforderlichen Objekte in der Gruppenrichtlinie mithilfe von Kaspersky Security Center erstellt werden, wird als Quelle des Installationspakets der freigegebene Ordner Kaspersky Security Center verwendet. Bei der Planung der Bereitstellung muss die Lesegeschwindigkeit aus diesem Ordner der Anzahl der Geräte und der Größe der zu installierenden Programmpakete entsprechen. Eventuell ist es zweckmäßig, den freigegebenen Ordner Kaspersky Security Center in einem leistungsfähigen spezialisierten Dateispeicher zu erstellen.

Neben der Einfachheit hat das automatische Erstellen der Windows-Gruppenrichtlinien mithilfe von Kaspersky Security Center noch einen Vorteil: bei der Planung der Installation des Administrationsagenten kann die Administrationsgruppe in Kaspersky Security Center, in welche die Geräte nach dem Abschließen der Installation automatisch verschoben werden, leicht angegeben werden. Die Gruppe kann im Assistenten für das Erstellen einer Aufgabe oder im Einstellungsfenster der Aufgabe zur Remote-Installation angegeben werden.

Bei der Arbeit mit den Windows-Gruppenrichtlinien mithilfe von Kaspersky Security Center erfolgt die Angabe der Geräte für das Gruppenrichtlinienobjekt mittels Erstellens einer Sicherheitsgruppe. Kaspersky Security Center synchronisiert die Zusammensetzung der Sicherheitsgruppe mit der aktuellen Geräteauswahl der Aufgabe. Bei Verwendung anderer Tools für die Arbeit mit den Gruppenrichtlinien können Sie Objekte von Gruppenrichtlinien direkt mit ausgewählten Organisationseinheiten eines Active Directory verbinden.

Selbstständige Installation von Apps mithilfe der Microsoft Windows-Richtlinien

Der Administrator kann in der Windows-Gruppenrichtlinie die für die Installation erforderlichen Objekte selbständig erstellen. In diesem Fall kann auf die Pakete verwiesen werden, die im freigegebenen Ordner Kaspersky Security Center liegen, oder die Pakete auf einem separaten Dateiserver entpacken und auf sie verweisen.

Es sind folgende Installationsszenarien möglich:

- Der Administrator erstellt das Installationspaket und passt dessen Eigenschaften in der Verwaltungskonsole an. Das Gruppenrichtlinienobjekt verweist auf die msi-Datei dieses Konfigurationspakets, die im freigegebenen Ordner Kaspersky Security Center liegt.

- Der Administrator erstellt das Installationspaket und passt dessen Eigenschaften in der Verwaltungskonsole an. Dann kopiert der Administrator den gesamten Unterordner EXEC dieses Pakets aus dem freigegebenen Ordner von Kaspersky Security Center in den Ordner auf der speziellen Dateiressource des Unternehmens. Das Gruppenrichtlinienobjekt verweist auf die msi-Datei dieses Pakets, die in einem Unterordner auf der spezialisierten Dateiressource des Unternehmens liegt.

- Der Administrator lädt das Programmpaket (einschließlich das des Administrationsagenten) aus dem Internet herunter und lädt es auf die vorgesehene Dateiressource des Unternehmens hoch. Das Gruppenrichtlinienobjekt verweist auf die msi-Datei dieses Pakets, die in einem Unterordner auf der spezialisierten Dateiressource des Unternehmens liegt. Das Anpassen der Installationseinstellungen erfolgt mittels Konfiguration der MSI-Eigenschaften oder der Konfiguration der MST-Transformationsdateien.

Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center

Um die erstmalige Bereitstellung des Administrationsagenten oder von anderen Anwendungen durchzuführen, können Sie die Installation der ausgewählten Installationspakete mithilfe der Aufgabe zur Remote-Installation von Kaspersky Security Center erzwingen. Voraussetzung dafür ist jedoch, das jedes Gerät über mindestens ein Benutzerkonto mit lokalen Administratorrechten verfügt.

Die erzwungene Installation kann auch verwendet werden, falls die Geräte nicht unmittelbar für den Administrationsserver verfügbar sind: wenn sich die Geräte beispielsweise in isolierten Netzwerken befinden oder wenn sich die Geräte im lokalen Netzwerk befinden und der Administrationsserver in der demilitarisierten Zone befindet.

Im Falle einer erstmaligen Bereitstellung ist noch kein Administrationsagent installiert. Daher können Sie in den Einstellungen der Aufgabe zur Remote-Installation nicht die Option auswählen, die zur Installation der Anwendung benötigten Dateien mithilfe des Administrationsagent zu verteilen. Sie können die Dateien lediglich unter Verwendung der Betriebssystemressourcen durch den Administrationsserver und die Verteilungspunkte verteilen.

Auf den Zielgeräten muss der Dienst des Administrationsservers unter einem Benutzerkonto mit Administratorrechten ausgeführt werden. Alternativ können Sie in den Einstellungen der Aufgabe zur Remote-Installation ein Benutzerkonto angeben, das Zugriff auf die Freigabe "admin$" hat.

> Standardmäßig wird Aufgabe zur Remote-Installation auf Geräte angewendet, indem die Anmeldedaten des Benutzerkontos, unter dem der Administrationsserver ausgeführt wird, verwendet werden. Es ist wichtig, zu beachten, dass es sich dabei um das Konto mit dem Zugriff auf die Freigabe "admin$" handelt, und nicht um das Konto, unter dem die Aufgabe zur Remote-Installation ausgeführt wird. Die Installation wird unter dem Benutzerkonto "LocalSystem" ausgeführt.

Angeben können Sie die Geräte entweder explizit (mittels Liste), indem Sie die Administrationsgruppe von Kaspersky Security Center auswählen, in der die Geräte enthalten sind, oder durch das Erstellen einer Geräteauswahl nach bestimmten Bedingungen. Der Startzeitpunkt der Installation wird durch den Zeitplan der Aufgabe bestimmt. Wenn in den Eigenschaften der Aufgabe die Einstellung **Übersprungene Aufgaben starten** aktiviert ist, kann die Aufgabe sofort bei der Aktivierung der Geräte oder bei ihrer Übertragung in die Ziel-Administrationsgruppe ausgeführt werden.

Die erzwungene Installation erfolgt mittels Übertragung der Installationspakete an die Zielgeräte, dem anschließenden Kopieren der Dateien in die admin$-Ressource der jeweiligen Geräte und der Remote-Anmeldung der Hilfsdienste auf diesen Geräten. Die Übertragung der Installationspakete an die Zielgeräte wird mithilfe der für die Netzwerkinteraktion verantwortlichen Funktion von Kaspersky Security Center ausgeführt. Dabei müssen die folgenden Bedingungen erfüllt werden:

- Die Zielgeräte können sowohl vom Administrationsserver als auch von den Verteilungspunkten erreicht werden.
- Die Namensauflösung für die Zielgeräte funktioniert im Netzwerk fehlerfrei.
- Die freigegebenen Administratorressourcen (admin$) verbleiben auf den Zielgeräten aktiviert.
- Die folgenden Systemdienste werden auf Zielgeräten ausgeführt:
  - Server (LanmanServer)

    Dieser Dienst wird standardmäßig ausgeführt.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- Der TCP-Port 445 ist auf den Zielgeräten geöffnet, um Remote-Zugriff über die Windows Management Instrumentation (WMI) zu ermöglichen.

  Außerdem wird der TCP-Port 445 überprüft, um das Betriebssystem des Zielgeräts zu bestimmen, bevor eine Remote-Installation ausgeführt wird (wenn der UDP-Port 137 nicht verfügbar ist).

  > TCP 139, UDP 137 und UDP 138 werden von älteren Protokollen verwendet und sind für aktuelle Anwendungen nicht mehr erforderlich.

  Um den Administrationsserver und die Verteilungspunkte mit den Zielgeräten zu verbinden, müssen in der Firewall dynamische Zugriffsports für ausgehende Daten erlaubt sein.
- Die Sicherheitseinstellungen der Active Directory-Domänenrichtlinie erlauben die Verwendung des NTLM-Protokolls während der Bereitstellung des Administrationsagenten.
- Auf Zielgeräten mit Microsoft Windows XP ist die einfache Dateifreigabe deaktiviert.
- Auf den Zielgeräten ist das Zugriffs- und Sicherheitsmodell auf den Wert *Klassisch – lokale Benutzer authentifizieren sich selbst* eingestellt. Der Wert *Nur Gäste – lokale Benutzer authentifizieren sich als Gast* ist nicht zulässig.
- Die Geräte sind Mitglieder der Domäne oder auf den Geräten wurden bereits einheitliche Benutzerkonten mit Administratorrechten erstellt.

Für die erfolgreiche Bereitstellung des Administrationsagenten oder einer anderen Anwendungen auf einem Gerät, das keiner Active Directory-Domäne von Windows Server 2003 oder höher gehört, müssen Sie die Remote-UAC auf diesem Gerät deaktivieren. Unter anderem aufgrund von Remote-UAC ist es lokalen Administratorkonten nicht möglich, auf die Freigabe "admin$" zuzugreifen. Für die erzwungene Bereitstellung des Administrationsagenten oder anderer Anwendungen ist dieser Zugriff ist jedoch erforderlich. Das Deaktivieren von Remote-UAC hat keine Auswirkungen auf die lokale UAC.

Bei der Installation auf neuen Geräten, die noch nicht in die Administrationsgruppen von Kaspersky Security Center verschoben wurden, kann in den Eigenschaften der Aufgabe zur Remote-Installation die Administrationsgruppe festgelegt werden, in welche die Geräte verschoben werden, nachdem die Installation des Administrationsagenten auf ihnen abgeschlossen wurde.

Beim Erstellen der Gruppenaufgabe muss berücksichtigt werden, dass die Gruppenaufgabe für die Geräte aller angelegten Untergruppen der ausgewählten Gruppe gilt. Deshalb sollten doppelte Installationsaufgaben in den Untergruppen vermieden werden.

Eine vereinfachte Methode zur Erstellung von Aufgaben für eine erzwungene Installation von Anwendungen ist die automatische Installation. Dazu müssen Sie in den Eigenschaften der Administrationsgruppe in der Liste der Installationspakete jene Pakete auswählen, die auf den Geräten dieser Gruppe installiert werden sollen. Daraufhin werden auf allen Geräten dieser Gruppe und ihrer Untergruppen die ausgewählten Installationspakete automatisch installiert. Der Zeitraum, während dem die Pakete installiert werden, hängt von der Netzwerkfähigkeit und der Gesamtmenge der Geräte im Netzwerk ab.

Um die Belastung des Administrationsservers während der Übertragung der Installationspaketen an die Zielgeräte zu reduzieren, können Sie in der Installationsaufgabe die Installationsmethode über Verteilungspunkte auswählen. Beachten Sie dabei, dass diese Installationsmethode eine höhere Belastung für jene Geräte bedeutet, die als Verteilungspunkte agieren. Es wird daher empfohlen, Geräte auszuwählen, die den Voraussetzungen für Verteilungspunkte entsprechen. Sie müssen bei der Verwendung von Verteilungspunkten sicherstellen, dass diese sich in all jenen isolierten Subnetzen befinden, in denen Zielgeräte gehostet werden.

Die Nutzung der Verteilungspunkte als lokale Installationszentren kann auch für die Installation auf Geräten in Subnetzen bequem sein, die mit dem Administrationsserver über einen engen Verbindungskanal verbunden sind, während zwischen den Geräten innerhalb des Subnetzes ein breiter Verbindungskanal verfügbar ist.

Die Größe des freien Speicherplatzes auf der Partition, in der sich der Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit befindet, muss den Gesamtumfang der Programmpakete der zu installierenden Anwendungen um ein Vielfaches übertreffen.

Start der von Kaspersky Security Center gebildeten autonomen Pakete

Die oben beschriebenen Methoden zur erstmaligen Bereitstellung des Administrationsagenten und der Apps können möglicherweise nicht immer durchgeführt werden, da nicht immer alle notwendigen Bedingungen erfüllt werden können. In solchen Fällen kann aus den vom Administrator vorbereiteten Installationspaketen mit den notwendigen Installationseinstellungen mithilfe von Kaspersky Security Center eine einheitliche ausführbare Datei erstellt werden, die als *autonomes Installationspaket* bezeichnet wird. Das autonome Installationspaket befindet sich im freigegebenen Ordner Kaspersky Security Center.

Mithilfe von Kaspersky Security Center kann den ausgewählten Benutzern per E-Mail ein Link auf diese Datei im freigegebenen Ordner mit der Bitte gesendet werden, die Datei auszuführen (interaktiv oder mit dem Parameter "-s" für die "Silent"-Installation). Das autonome Installationspaket kann an eine E-Mail-Nachricht für die Benutzer von Geräten, die keinen Zugriff auf den freigegebenen Ordner Kaspersky Security Center haben, angehängt werden. Der Administrator kann das autonome Paket auf einen Wechseldatenträger kopieren, es an das relevante Gerät liefern und dann später ausführen.

Das autonome Paket kann aus dem Paket des Administrationsagenten, dem Paket anderer Apps (beispielsweise der Sicherheitsanwendung) oder sofort aus beiden Paketen erstellt werden. Wenn das autonome Paket aus dem Administrationsagenten und aus anderen Apps erstellt wurde, beginnt die Installation mit dem Administrationsagenten.

Beim Erstellen des autonomen Paketes mit dem Administrationsagenten kann die Administrationsgruppe angegeben werden, in welche die neuen Geräte (kein Bestandteil der Administrationsgruppen) automatisch nach Abschluss der Installation des Administrationsagenten verschoben werden.

Die autonomen Pakete können interaktiv (standardmäßig), mit Anzeige des Installationsergebnisses der zugehörigen Apps oder im Silent-Modus (beim Start mit dem Parameter "-s") ausgeführt werden. Der Silent-Modus kann für die Installation aus bestimmen Skripts (beispielsweise aus Skripts, die für den Start nach Abschluss der Bereitstellung des Betriebssystem-Images angepasst werden, und ähnliches) verwendet werden. Das Installationsergebnis des Silent-Modus wird durch den Rückgabecode des Prozesses definiert.

Der eigenständige Administrationsagent für Linux besitzt eine optionale Abhängigkeit vom Tool "nmap". Wenn das nmap-Tool fehlt oder älter als die Version 6.0 ist, wird die Funktion "Broadcast DHCP Discover" nicht unterstützt.

Funktion zur manuellen Installation von Apps

Administratoren oder erfahrene Benutzer können die Apps manuell im Interaktivmodus installieren. Dabei können sowohl die originalen Programmpakete als auch die aus ihnen gebildeten Installationspakete verwendet werden, die sich im freigegebenen Ordner Kaspersky Security Center befinden. Die Installer arbeiten standardmäßig im Interaktivmodus und fragen vom Benutzer alle notwendigen Einstellungswerte ab. Beim Start des Prozesses setup.exe aus dem Stamminstallationspaket mit dem Parameter "-s" wird der Installer im Silent-Modus jedoch mit den Einstellungen ausgeführt, die in den Einstellungen des Installationspakets festgelegt wurden.

Beim Start von setup.exe aus dem Stamminstallationspakets, das sich im freigegebenen Ordner Kaspersky Security Center befindet, wird das Pakets zuerst in den temporären lokalen Ordner kopiert und dann aus der lokalen Hilfe der Installer der App gestartet.

Eine MST-Datei erstellen

Um den Inhalt eines MSI-Pakets umzuwandeln und benutzerdefinierte Einstellungen auf eine vorhandene MSI-Datei anzuwenden, müssen Sie eine Transformationsdatei im MST-Format erstellen. Verwenden Sie dafür den in der Windows SDK enthaltenen Editor "Orca.exe".

So erstellen Sie eine MST-Datei:

1. Starten Sie den Editor "Orca.exe".
2. Gehen Sie zur Registerkarte **Datei** und klicken Sie auf **Öffnen**.
3. Wählen Sie die Datei "Kaspersky Network Agent.msi" aus.
4. Wechseln Sie zur Registerkarte **Transformation** und wählen Sie anschließend im Menü **New transformation**.
5. Wählen Sie in der Spalte **Tabellen** den Punkt **Eigenschaft** aus und geben Sie die folgenden Werte ein:
   - *EULA=1*
   - *SERVERADDRESS=<Adresse des Administrationsservers>*

   Klicken Sie auf **Speichern**.
6. Wechseln Sie zur Registerkarte **Transform** und wählen Sie anschließend im Menü **Generate Transform**.
7. Geben Sie im neuen Fenster einen Namen für die zu erstellende Transformationsdatei an und klicken Sie auf **Speichern**.

Die MST-Datei wird gespeichert.

Remote-Installation von Apps auf Geräte mit installiertem Administrationsagenten

Wenn auf dem Gerät ein arbeitsfähiger Administrationsagent installiert ist, der mit dem primären Administrationsserver oder einen seiner sekundären Server verbunden ist, kann auf diesem Gerät die Version des Administrationsagenten aktualisiert werden sowie mithilfe des Administrationsagenten beliebige unterstützte Apps installiert, aktualisiert oder gelöscht werden.

Sie können Option **Unter Nutzung des Administrationsagenten** in den Eigenschaften der Aufgabe zur Remote-Installation aktivieren.

Wenn diese Option ausgewählt ist, erfolgt die Übertragung der Installationspakete auf die Geräte mit den vom Administrator festgelegten Installationseinstellungen über die Verbindungskanäle zwischen dem Administrationsagenten und dem Administrationsserver.

Zur Optimierung der Belastung auf dem Administrationsserver und zur Verringerung des Datenverkehrs zwischen dem Administrationsserver und den Geräten ist es sinnvoll, in jedem Remote-Netzwerk bzw. in jeder Broadcast-Domäne Verteilungspunkte zu bestimmen (s. Abschnitte Über Verteilungspunkte und Aufbau der Struktur von Administrationsgruppen und Zuweisung von Verteilungspunkten). In diesem Fall erfolgt die Verteilung der Installationspakete und der Einstellungen des Installers vom Administrationsserver auf die Geräte über die Verteilungspunkte.

Unter Verwendung der Verteilungspunkte können auch Broadcast-Domänen (Multicast) den Mailversand der Installationspakete ausführen, wodurch der Netzwerkverkehr während der Bereitstellung der Programme erheblich verringert werden kann.

Bei der Übertragung der Installationspakete auf die Geräte über die Verbindungskanäle zwischen den Administrationsagenten und dem Administrationsserver, werden die zur Sendung vorbereiteten Installationspakete zusätzlich im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer zwischengespeichert. Bei Verwendung einer hohen Anzahl verschiedener Installationspakete mit großem Umfang und bei einer großen Menge von Verteilungspunkten kann die Größe dieses Ordners erheblich zunehmen.

Die Dateien aus dem Ordner FTServer dürfen nicht manuell gelöscht werden. Beim Löschen der Ausgangsinstallationspakete werden die entsprechenden Daten automatisch aus dem Ordner FTServer gelöscht.

Die Daten, die von den Verteilungspunkten übernommen werden, werden im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp gespeichert.

Die Dateien aus dem Ordner FTCITmp dürfen nicht manuell gelöscht werden. Je nach Abschluss der Aufgaben, von denen die Daten aus dem Ordner verwendet werden, wird der Inhalt dieses Ordners automatisch gelöscht.

Da die Installationspakete im für das Netzwerk optimalen Format für die Übertragung über die Verbindungskanäle zwischen dem Administrationsserver und den Administrationsagenten aus dem Zwischenspeicher bewegen, dürfen keine Änderungen an den Installationspaketen im ursprünglichen Ordner des Installationspakets vorgenommen werden. Solche Änderungen werden vom Administrationsserver nicht automatisch berücksichtigt. Wenn die Dateien der Installationspakete manuell geändert werden müssen (obwohl das nicht empfohlen wird), müssen unbedingt irgendwelche Einstellungen des Installationspakets in der Verwaltungskonsole geändert werden. Die Änderung der Einstellungen des Installationspakets in der Verwaltungskonsole zwingt den Administrationsserver, das Image des Pakets im Cache zu aktualisieren, das für die Sendung auf die Geräte vorbereitet wurde.

Verwaltung des Neustarts von Geräten in der Aufgabe zur Remote-Installation

Oft wird für den Abschluss der Remote-Installation der App (besonders auf der Plattform Windows) ein Neustart des Geräts gefordert.

Wenn die Aufgabe zur Remote-Installation von Kaspersky Security Center verwendet wird, kann im Assistenten für das Erstellen einer Aufgabe oder im Eigenschaftenfenster der erstellten Aufgabe (Abschnitt **Neustart des Betriebssystems**) die Maßnahme für einen erforderlichen Neustart ausgewählt werden:

- **Gerät nicht neu starten**. In diesem Fall wird kein automatischer Neustart ausgeführt. Für das Abschließen der Installation ist es erforderlich, das Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung der Geräte) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Installationsaufgaben auf Servern und anderen Geräten, für die Störungen während des Arbeitsablaufs kritisch sind.

- **Das Gerät neu starten**. In diesem Fall wird der Neustart immer automatisch ausgeführt, wenn für das Abschließen der Installation ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben zur Installation auf Geräten, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**. In diesem Fall informiert eine Meldung auf dem Client-Gerät den Benutzer darüber, dass das Gerät manuell neu gestartet werden muss. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Die Variante **Benutzer fragen** eignet sich besonders für Workstations, deren Benutzer die Möglichkeit haben sollen, den passendsten Moment für den Neustart auszuwählen.

Zweckdienlichkeit des Datenbanken-Updates im Installationspaket der Sicherheitsanwendung

Vor Beginn der Bereitstellung des Schutzes muss die Möglichkeit eines Updates der Antiviren-Datenbanken (einschließlich der Autopatch-Module), die zusammen mit dem Programmpaket der Sicherheitsanwendung bereitgestellt werden, berücksichtigt werden. Es ist zweckmäßig, vor Beginn der Bereitstellung die Datenbanken aus dem Bestand des Installationspakets der App (beispielsweise mithilfe des entsprechenden Befehls im Kontextmenü des ausgewählten Installationspakets) zu aktualisieren. Dadurch wird die Anzahl der Neustarts verringert, die für den Abschluss der Bereitstellung des Schutzes auf den Geräten erforderlich sind.

Verwendung von Tools zur Remote-Installation der Apps von Kaspersky Security Center für den Start von beliebigen ausführbaren Dateien auf den verwalteten Geräten

Mithilfe des Assistenten für das Erstellen eines Installationspakets kann eine beliebige ausführbare Datei ausgewählt und dafür die Befehlszeilenparameter festlegt werden. Dabei können im Installationspaket sowohl die ausgewählte Datei als auch der gesamte Ordner, in dem diese Datei enthalten ist, untergebracht werden. Anschließend muss die Aufgabe zur Remote-Installation erstellt und das erstellte Installationspaket ausgewählt werden.

Während der Ausführung der Aufgabe auf den Geräten wird die beim Erstellen angegebene ausführbare Datei mit den aufgegebenen Befehlszeilenparametern ausgeführt.

Wenn Installer im Format Microsoft Windows Installer (MSI) verwendet werden, verwendet Kaspersky Security Center die Standardmöglichkeiten gemäß der Analyse des Installationsergebnisses.

Wenn eine Lizenz für Schwachstellen- und Patch-Management vorhanden ist, verwendet Kaspersky Security Center beim Erstellen des Installationspakets für eine der unterstützten Apps, die in der Unternehmensumgebung verteilt sind, auch die Regeln zur Installation und Analyse der Installationsergebnisse, die in der aktualisierten Datenbank vorhanden sind.

In allen anderen Fälle wartet die Aufgabe bei ausführbaren Dateien standardmäßig auf den Abschluss des ausgeführten Prozesses und aller dadurch generierten untergeordneten Prozesse. Nach dem Abschluss der ausgeführten Prozesse wird die Aufgabe unabhängig vom Rückgabecode des Ausgangsprozesses erfolgreich beendet. Um ein solches Verhalten der Aufgabe zu ändern, müssen vor dem Erstellen der Aufgabe die kpd-Dateien, die von Kaspersky Security Center im Ordner des neu erstellten Installationspakets, sowie dessen Unterordnern, erzeugt wurden, manuell geändert werden.

Für .kpd-Dateien wird die ASCII-Kodierung verwendet, während für .kud-Dateien die Unicode-Kodierung verwendet wird.

Damit die Aufgabe den Abschluss des ausgeführten Prozesses nicht abwartet, muss im Abschnitt [SetupProcessResult] für die Einstellung Wait der Wert 0 festgelegt werden:

```
[SetupProcessResult]
Wait=0
```

Damit die Aufgabe auf der Windows-Plattform nur den Abschluss des Ausgangsprozesses, aber nicht der von ihm erzeugten untergeordneten Prozesse abwartet, muss in Abschnitt [SetupProcessResult] für die Einstellung WaitJob der Wert 0 festgelegt werden, zum Beispiel:

```
[SetupProcessResult]
WaitJob=0
```

Damit die Aufgabe erfolgreich abgeschlossen wird oder je nach Rückgabecode des laufenden Prozesses einen Fehler ausgibt, erstellen Sie eine ausführbare .bat-Datei, die den Fehlercode in einer Datei speichert, zum Beispiel:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Ändern Sie anschließend außerdem die .kud-Dateien, die von Kaspersky Security Center im Ordner des neu erstellten Installationspakets generiert wurden:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

In diesem Fall wird ein beliebiger, sich von den aufgezählten unterscheidender, Code auf einen Fehler hindeuten.

Damit in den Ergebnissen der Aufgabe eine Zeile mit einem Kommentar über den erfolgreichen Abschluss der Aufgabe bzw. der Fehlerdiagnose angezeigt wird, müssen in den Abschnitten [SetupProcessResult_SuccessCodes] und [SetupProcessResult_ErrorCodes] kurze Fehlerbeschreibungen, die den Rückgabecodes des Prozesses entsprechen, festgelegt werden, zum Beispiel:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

Damit die Tools von Kaspersky Security Center zur Verwaltung des Neustarts des Geräts eingesetzt werden können (wenn ein Neustart für den Abschluss der Operation erforderlich ist), müssen im Abschnitt [SetupProcessResult_NeedReboot] zusätzlich die Rückgabecodes des Prozesses, die einen erforderlichen Neustart bedeuten, aufgezählt werden:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitoring der Bereitstellung

Zur Kontrolle der Bereitstellung von Kaspersky Security Center sowie zur Überprüfung auf eine vorhandene Sicherheitsanwendung auf den verwalteten Geräten und des Administrationsagenten, müssen die farblichen Kennzeichnungen im Block **Bereitstellung** beachtet werden. Die Kennzeichnung befindet sich im Arbeitsbereich des Administrationsserver-Knotens im Hauptfenster der Verwaltungskonsole. Die Kennzeichnung zeigt aktuellen Status der Bereitstellung an. Neben der Kennzeichnung wird die Anzahl der Geräte mit installiertem Administrationsagenten und Sicherheitsanwendungen angezeigt. Bei vorhandenen aktiven Installationsaufgaben wird der Ausführungsfortschritt der Aufgaben angezeigt. Bei etwaigen Installationsfehlern wird die Anzahl der Fehler angezeigt und über einen Link besteht die Möglichkeit zur Anzeige ausführlichen Informationen über den Fehler. Farbliche Kennzeichnungen in der Verwaltungskonsole.

Es gibt ferner die Möglichkeit, im Arbeitsbereich des Ordners **Verwaltete Geräte** auf der Registerkarte **Gruppen** ein Diagramm der Bereitstellung anzuzeigen. Das Diagramm gibt den Verteilungsprozess wieder, indem es die Anzahl der Geräte ohne Administrationsagent, mit Administrationsagent, und mit Administrationsagenten und Sicherheitsanwendung anzeigt.

Eine ausführlichere Beschreibung des Verlaufs der Bereitstellung (bzw. der Ausführung einer konkreten Installationsaufgabe) wird im Ergebnisfenster für die Ausführung der entsprechenden Aufgabe der Remote-Installation angezeigt. Das Ergebnisfenster ist über das Kontextmenü der Aufgabe (Punkt **Ergebnisse**) verfügbar. Im Fenster werden zwei Listen angezeigt: die obere Liste enthält eine Auflistung der Status der Aufgabe auf den Geräten, und in der unteren wird die Ereignisliste für die Aufgabe auf dem Gerät angezeigt, das in der oberen Liste derzeit ausgewählt ist.

Die Informationen über Fehler bei der Bereitstellung werden im Kaspersky-Ereignisprotokoll des Administrationsservers gespeichert. Die Informationen über die Fehler sind auch in der entsprechenden Ereignisauswahl im Knoten des Administrationsservers auf der Registerkarte **Ereignisse** verfügbar.

Anpassen der Einstellungen der Installer

Dieser Abschnitt enthält Informationen über die Dateien der Installer von Kaspersky Security Center und die Installationseinstellungen sowie Empfehlung zur Installation des Administrationsservers und des Administrationsagenten im Silent-Modus.

Allgemeine Informationen

Die Installer von Kaspersky Security Center 15.1 (Administrationsserver, Administrationsagent, Verwaltungskonsole) sind auf der Technologie des Windows Installers aufgebaut. Der Kern des Installers ist das MSI-Paket. Dieses Verpackungsformat der Distribution erlaubt, alle Vorteile der Windows Installer-Technologie zu verwenden: die Skalierbarkeit, die Möglichkeit von System-Patches, das System der Transformation, die Möglichkeit einer zentralisierten Installation von Drittanbieter-Lösungen, die Transparenz der Anmeldung im Betriebssystem.

Installation im Silent-Modus (mit Antwortdatei)

In den Installern des Administrationsservers und des Administrationsagenten gibt es die Möglichkeit zur Verwendung der Antwortdatei (ss_install.xml), in der die Parameter für die Installation im Silent-Modus ohne Benutzerinteraktion gespeichert sind. Die Datei ss_install.xml befindet sich im selben Ordner wie das msi-Paket und wird automatisch bei der Installation im Silent-Modus verwendet. Sie können die Installation im Silent-Modus mit dem Befehlszeilenparameter "/ s" aktivieren.

Beispiel für den Start:

```
setup.exe /s
```

Lesen Sie den Endbenutzer-Lizenzvertrag (EULA), bevor Sie das Installationsprogramm im Silent-Modus starten. Wenn das Programmpaket von Kaspersky Security Center keine txt-Datei mit dem Text der EULA enthält, können Sie die Datei auf der Website von Kaspersky herunterladen.

Die Datei ss_install.xml stellt eine Instanz des internen Formats für die Parameter des Installers für Kaspersky Security Center dar. Im Lieferumfang der Programmpakete wird die Datei ss_install.xml mit den Standardparametern geliefert.

Die Datei ss_install.xml darf nicht manuell geändert werden. Diese Datei wird mithilfe von Kaspersky Security Center bei der Änderung der Parameter der Installationspakete in der Verwaltungskonsole geändert.

So ändern Sie die Antwortdatei für die Installation des Administrationsservers:

1. Öffnen Sie das Programmpaket von Kaspersky Security Center. Wenn Sie eine exe-Datei für das Komplettpaket verwenden, entpacken Sie diese.

2. Öffnen Sie ausgehend vom Server-Ordner die Befehlszeile und führen Sie anschließend den folgenden Befehl aus:
   ```
   setup.exe /r ss_install.xml
   ```
   Das Installationsprogramm von Kaspersky Security Center wird gestartet.

3. Folgen Sie den Schritten des Assistenten, um die Installation von Kaspersky Security Center zu konfigurieren.

   Wenn Sie den Assistenten abschließen, wird die Antwortdatei automatisch gemäß den neuen Einstellungen geändert, die Sie angegeben haben.

Installation des Administrationsagenten im Silent-Modus (ohne Antwortdatei)

Der Administrationsagent kann nur mithilfe eines msi-Pakets installiert werden, dabei werden die Werte der MSI-Eigenschaften MSI standardmäßig festgelegt. Ein solches Szenario erlaubt, den Administrationsagenten unter Verwendung von Gruppenrichtlinien zu installieren.

Benennen Sie das Installationspaket "Kaspersky Network Agent.msi" nicht um. Ein Umbenennen dieses Pakets kann bei zukünftigen Updates des Administrationsagenten zu Installationsfehlern führen.

Damit kein Konflikt zwischen den Parametern, die mithilfe der MSI-Eigenschaften festgelegt wurden, und den Parametern, die in der Antwortdatei festgelegt sind, entsteht, kann die Antwortdatei mittels Angabe der Eigenschaft `DONT_USE_ANSWER_FILE=1` deaktiviert werden. Die msi-Datei befindet sich im Programmpaket für Kaspersky Security Center im Ordner Packages\NetAgent\exec. Nachfolgend ist ein Beispiel für den Start des Installers des Administrationsagenten mithilfe des msi-Paketes angeführt.

Für die Installation des Administrationsagenten im Silent-Modus müssen die Bedingungen des Endbenutzer-Lizenzvertrags akzeptiert werden. Verwenden Sie den Parameter `EULA=1` nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen haben, und sie verstehen und akzeptieren.

Beispiel:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Sie können die Parameter zur Installation des msi-Paketes auch festlegen, indem Sie eine temporäre Transformationsdatei vorbereiten (Datei mit der Erweiterung mst). Der Befehl sieht folgendermaßen aus:

Beispiel:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

In einem Befehl können mehrere Transformationsdateien angegeben werden.

Wenn Sie den Administrationsagenten mithilfe von Windows Installer aktualisieren möchten, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Teilweises Anpassen der Installationseinstellungen durch setup.exe

Beim Start der Programminstallation mittels setup.exe können die Werte beliebiger MSI-Eigenschaften ins msi-Paket übergeben werden.

Der Befehl sieht folgendermaßen aus:

Beispiel:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Installationseinstellungen für den Administrationsserver

In der nachfolgenden Tabelle werden die MSI-Eigenschaften beschrieben, die bei der Installation des Administrationsservers angepasst werden können. Alle Parameter mit Ausnahme von EULA und PRIVACYPOLICY sind optional.

MSI-Eigenschaft	Beschreibung	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Lizenzvertrags (obligatorische Einstellung)	• 1 – Ich habe die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen, und verstehe und akzeptiere sie. • Anderer Wert oder keine Angabe – die Bedingungen des Endbenutzer-Lizenzvertrags werden abgelehnt (die Installation wird nicht ausgeführt).
PRIVACYPOLICY	Einverständnis mit den Bedingungen der Datenschutzrichtlinie (obligatorische Einstellung)	• 1 – Mir ist bewusst und ich bin damit einverstanden, dass meine Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Ich bestätige, dass ich die Datenschutzrichtlinie vollständig gelesen habe und sie verstehe. • Anderer Wert oder keine Angabe – die Bedingungen der Datenschutzrichtlinie werden abgelehnt (die Installation wird nicht ausgeführt).
INSTALLATIONMODETYPE	Installationstyp für den Administrationsserver	• Standard. • Benutzerdefiniert.
INSTALLDIR	Ordner der Programminstallation	Zeichenfolgenwert.
ADDLOCAL	Liste der Installationskomponenten (kommagetrennt)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Liste der Komponenten, die als Mindestvoraussetzungen für eine korrekte Installation des Administrationsservers gelten: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Netzwerkgröße	• NRT_1_100 – von 1 bis 100 Geräte • NRT_100_1000 – von 101 bis 1.000 Geräte • NRT_GREATER_1000 – mehr als 1.000 Geräte
SRV_ACCOUNT_TYPE	Art der Angabe des Benutzers für die Ausführung des Dienstes des Administrationsservers	• SrvAccountDefault – das Benutzerkonto wird automatisch erstellt. • SrvAccountUser – das Benutzerkonto wird manuell festgelegt.
SERVERACCOUNTNAME	Benutzername für den Dienst	Zeichenfolgenwert.
SERVERACCOUNTPWD	Benutzerkennwort für den Dienst	Zeichenfolgenwert.
DBTYPE	Typ der Datenbank	• MySQL – Eine MySQL- oder MariaDB-Datenbank wird verwendet. • MSSQL – Eine Datenbank des Typs Microsoft SQL Server (SQL Express) wird verwendet.
MYSQLSERVERNAME	Vollständiger Name des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MYSQLSERVERPORT	Portnummer für die Verbindung mit dem MySQL- oder MariaDB-Server	Zahlenwert.
MYSQLDBNAME	Name der Datenbank des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MYSQLACCOUNTNAME	Benutzername für die Verbindung mit der Datenbank des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MYSQLACCOUNTPWD	Benutzerkennwort für die Verbindung mit der Datenbank des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MSSQLCONNECTIONTYPE	Verwendungstyp der MSSQL-Datenbank	• InstallMSSEE – aus einem Paket installieren. • ChooseExisting – installierten Server verwenden.
MSSQLSERVERNAME	Vollständiger Name der SQL Server-Instanz	Zeichenfolgenwert.
MSSQLDBNAME	Name der Datenbank von SQL Server	Zeichenfolgenwert.
MSSQLAUTHTYPE	Authentifizierungsmethode bei der Verbindung mit SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Benutzername für die Verbindung zu SQL Server im Modus SQLServer	Zeichenfolgenwert.

MSI-Eigenschaft	Beschreibung	Mögliche Werte
MSSQLACCOUNTPWD	Benutzerkennwort für die Verbindung zu SQL Server im Modus SQLServer	Zeichenfolgenwert.
CREATE_SHARE_TYPE	Methode zum Erstellen eines gemeinsamen Ordners	• Create – neuen freigegebenen Ordner erstellen. In diesem Fall müssen folgende Eigenschaften festgelegt werden: • SHARELOCALPATH – Pfad zu einem lokalen Ordner. • SHAREFOLDERNAME – Netzwerkname eines Ordners. • Null – die Eigenschaft EXISTSHAREFOLDERNAME muss festgelegt werden.
EXISTSHAREFOLDERNAME	Vollständiger Name eines vorhandenen gemeinsamen Ordners	Zeichenfolgenwert.
SERVERPORT	Portnummer für das Herstellen einer Verbindung mit dem Administrationsserver	Zahlenwert.
SERVERSSLPORT	Port für die Installation der SSL-Verbindung mit dem Administrationsserver	Zahlenwert.
SERVERADDRESS	Adresse des Administrationsservers	Zeichenfolgenwert.
SERVERCERT2048BITS	Die Lange des Schlüssels für das Zertifikat des Administrationsservers (in Bits)	• 1 – die Länge des Schlüssels für das Zertifikat des Administrationsservers beträgt 2048 Bit. • 0 – die Länge des Schlüssels für das Zertifikat des Administrationsservers beträgt 1024 Bit. • Wenn kein Wert angegeben ist, beträgt die Länge des Schlüssels für das Zertifikat des Administrationsservers 2.024 Bit.
MOBILESERVERADDRESS	Adresse des Administrationsservers zum Verbinden mit mobilen Geräten; wird ignoriert, wenn die Komponente "MobileSupport" nicht ausgewählt ist	Zeichenfolgenwert.

Installationseinstellungen für den Administrationsagenten

In der nachfolgenden Tabelle werden die MSI-Eigenschaften beschrieben, die bei der Installation des Administrationsagenten angepasst werden können. Alle Parameter mit Ausnahme von EULA und SERVERADDRESS sind optional.

Einstellungen für die Installation des Administrationsagenten im Silent-Modus

MSI-Eigenschaft	Beschreibung	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Lizenzvertrags	• 1 – Ich bestätige, dass ich die Bestimmungen und Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe und sie verstehe und akzeptiere. • 0 – Ich lehne die Bedingungen des Endbenutzer-Lizenzvertrags ab (die Installation wird nicht ausgeführt). • Kein Wert – Ich lehne die Bedingungen des Endbenutzer-Lizenzvertrags ab (die Installation wird nicht ausgeführt).
DONT_USE_ANSWER_FILE	Installationseinstellungen aus der Antwortdatei lesen	• 1—Nicht verwenden. • Anderer Wert oder keine Angabe – Lesen.
INSTALLDIR	Pfad des Installationsordners für den Administrationsagenten	Zeichenfolgenwert.
SERVERADDRESS	Adresse des Administrationsservers (obligatorische Einstellung)	Zeichenfolgenwert.
SERVERPORT	Port zum Herstellen einer Verbindung mit dem Administrationsserver	Zahlenwert.

MSI-Eigenschaft	Beschreibung	Mögliche Werte
SERVERSSLPORT	Portnummer für das Herstellen einer sicheren Verbindung mit dem Administrationsserver über das SSL-Protokoll	Zahlenwert.
USESSL	Soll eine SSL-Verbindung verwendet werden?	• 1 – verwenden • Anderer Wert oder keine Angabe – nicht verwenden
OPENUDPPORT	Soll ein UDP-Port geöffnet werden?	• 1 – öffnen • Anderer Wert oder keine Angabe – öffnen
UDPPORT	UDP-Port	Zahlenwert.
USEPROXY	Soll ein Proxyserver verwendet werden? Aus Kompatibilitätsgründen wird es nicht empfohlen, die Einstellungen der Proxy-Verbindung in den Einstellungen des Installationspakets für den Administrationsagenten festzulegen.	• 1 – verwenden • Anderer Wert oder keine Angabe – nicht verwenden
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Proxyadresse und Portnummer für die Verbindung mit dem Proxyserver	Zeichenfolgenwert.
PROXYLOGIN	Benutzerkonto zur Verbindung mit dem Proxyserver.	Zeichenfolgenwert.
PROXYPASSWORD	Kennwort des Benutzerkontos für die Verbindung mit dem Proxyserver (Geben Sie in den Einstellungen von Installationspaketen keine Details über privilegierten Benutzerkonten an.)	Zeichenfolgenwert.
GATEWAYMODE	Modus für die Nutzung eines Verbindungs-Gateways	• 0 – Verbindungs-Gateway nicht verwenden • 1 – Als Verbindungs-Gateway wird der betreffende Administrationsagent verwendet • 2 – Verbindung mit dem Administrationsserver über das Verbindungs-Gateway herstellen
GATEWAYADDRESS	Verbindungs-Gateway-Adresse	Zeichenfolgenwert.
CERTSELECTION	Methode zum Anfordern eines Zertifikats	• GetOnFirstConnection – Zertifikat vom Administrationsserver anfordern • GetExistent – Vorhandenes Zertifikat auswählen. Wenn diese Variante ausgewählt ist, muss die Eigenschaft CERTFILE angegeben sein
CERTFILE	Pfad der Zertifikatsdatei	Zeichenfolgenwert.
VMVDI	Dynamischen Modus für Virtual Desktop Infrastructure (VDI) aktivieren	• 1 – aktivieren. • 0 – Nicht aktivieren. • Kein Wert – nicht aktivieren.
VMOPTIMIZE	Gibt an, ob die Einstellungen des Administrationsagenten für den Hypervisor optimal sind.	• 1 – aktivieren. • 0 – Nicht aktivieren. • Kein Wert – nicht aktivieren.
LAUNCHPROGRAM	Gibt an, ob nach der Installation der Dienst des Administrationsagenten gestartet werden soll. Bei "VMVDI=1" wird der Parameter ignoriert.	• 1 – starten • anderer Wert oder keine Angabe – nicht starten
NAGENTTAGS	Tag für den Administrationsagenten (hat eine höhere Priorität als das Tag aus der Antwortdatei)	Zeichenfolgenwert.

Virtuelle Infrastruktur

Kaspersky Security Center unterstützt die Arbeit mit virtuellen Maschinen. Sie können den Administrationsagenten und die Sicherheitsanwendungen auf jeder virtuellen Maschine installieren und virtuelle Maschinen auf Hypervisor-Ebene schützten. Im ersten Fall kann sowohl die Standard-Sicherheitsanwendung als auch Kaspersky Security for Virtualization Light Agent für den Schutz der virtuellen Maschinen verwendet werden. Im zweiten Fall kann Kaspersky Security for Virtualization Agentless verwendet werden.

Kaspersky Security Center unterstützt das Rollback von virtuellen Maschinen auf ihren vorherigen Zustand.

Empfehlungen zur Senkung der Belastung auf den virtuellen Maschinen

Wenn der Administrationsagent auf einer virtuellen Maschine installiert wird, muss eine Möglichkeit zum Deaktivieren jenes Teils der Funktionalität von Kaspersky Security Center vorgesehen werden, der für die virtuellen Maschinen von geringem Wert ist.

Bei der Installation des Administrationsagenten auf einer virtuellen Maschine oder einer Vorlage, aus der virtuelle Maschinen erstellt werden sollen, ist es empfehlenswert, wie folgt vorzugehen:

- Wenn eine Remote-Installation ausgeführt wird, wählen Sie im Eigenschaftenfenster für das Installationspaket des Administrationsagenten im Abschnitt **Erweitert** die Option **Einstellungen für VDI optimieren** aus.
- Wenn mithilfe des Assistenten eine interaktive Installation ausgeführt wird, wählen Sie im Fenster des Assistenten die Option **Einstellungen des Administrationsagenten für die virtuelle Infrastruktur optimieren** aus.

Durch Auswählen der Optionen werden die Einstellungen des Administrationsagenten so geändert, dass standardmäßig die folgenden Funktionen deaktiviert werden (bevor eine Richtlinie angewendet wird):

- Informationen über die installierte Software empfangen
- Informationen über die Hardware empfangen
- Informationen über vorhandene Schwachstellen empfangen
- Informationen über erforderliche Updates empfangen

Üblicherweise müssen die aufgezählten Funktionen auf den virtuellen Maschinen nicht aktiviert sein, damit die Software und die virtuelle Hardware darauf einheitlich sind.

Das Deaktivieren der Funktionen kann rückgängig gemacht werden. Wenn eine der deaktivierten Funktionen doch erforderlich ist, kann sie mithilfe der Richtlinie des Administrationsagenten oder in den lokalen Einstellungen des Administrationsagenten aktiviert werden. Die lokalen Einstellungen des Administrationsagenten sind über das Kontextmenü des entsprechenden Geräts in der Verwaltungskonsole verfügbar.

Unterstützung von dynamischen virtuellen Maschinen

Kaspersky Security Center unterstützt dynamische virtuelle Maschinen. Wenn im Netzwerk des Unternehmens eine virtuelle Infrastruktur implementiert ist, können in einigen Fällen dynamische (temporärer) virtuellen Maschinen verwendet werden. Solche Maschinen werden mit eindeutigen Namen aus einer vom Administrator im Voraus vorbereiteten Vorlage erstellt. Der Benutzer arbeitet eine gewisse Zeit auf einer VM und nach dem Deaktivieren wird die virtuelle Maschinen aus der virtuellen Infrastruktur entfernt. Wenn im Netzwerk des Unternehmens Kaspersky Security Center implementiert ist, wird die virtuelle Maschine mit darauf installiertem Administrationsagenten zur Administrationsserver-Datenbank hinzugefügt. Nach dem Deaktivieren der virtuellen Maschine muss der sie betreffende Eintrag auch aus der Datenbank des Administrationsservers gelöscht werden.

Damit die Funktionalität des automatischen Löschens der Einträge über virtuelle Maschinen bei der Installation des Administrationsagenten auf der Vorlage, aus der die dynamischen virtuellen Maschinen erstellt werden, funktioniert, muss die Option **Dynamischen Modus für VDI aktivieren** aktiviert werden:

- Im Falle einer Remote-Installation im Eigenschaftenfenster des Installationspakets des Administrationsagenten (Abschnitt **Erweitert**)
- Für die interaktive Installation – im Installationsassistenten des Administrationsagenten

Die Option **Dynamischen Modus für VDI aktivieren** muss bei der Installation des Administrationsagenten auf realen Geräten nicht aktiviert werden.

Wenn es erforderlich ist, dass Ereignisse auf dynamischen virtuellen Maschinen eine bestimmte Zeit nach dem Löschen der Maschinen auf dem Administrationsserver gespeichert werden, muss im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignis-Datenverwaltung** die Option **Ereignisse von gelöschten Geräten weiterhin speichern** aktiviert und die maximale Speicherdauer der Ereignisse in Tagen angegeben werden.

Es wird davon abgeraten, die Verschlüsselung von Laufwerken auf dynamischen virtuellen Maschinen zu aktivieren.

Unterstützung des Kopierens von virtuellen Maschinen

Das Kopieren von virtuellen Maschine mit darauf installiertem Administrationsagenten oder deren Erstellung aus einer Vorlage mit installiertem Administrationsagenten entspricht der Bereitstellung der Administrationsagenten durch Aufzeichnen und Kopieren eines Festplatten-Image. Deshalb muss man im Allgemeinen beim Kopieren von virtuellen Maschinen dieselbe Aktion ausführen wie bei der Bereitstellung des Administrationsagenten durch Kopieren eines Images der Festplatte.

In den nachstehend beschriebenen beiden Fällen erkennt der Administrationsagent die Tatsache des Kopierens allerdings automatisch. Deshalb ist die Ausführung der komplizierten Aktionen, die in im Abschnitt "die Bereitstellung durch Aufzeichnen und Kopieren der Festplatte des Geräts" nicht obligatorisch:

- Bei der Installation des Administrationsagenten war die Option **Dynamischen Modus für VDI aktivieren** aktiviert: nach jedem Neustart des Betriebssystems wird eine solche virtuelle Maschine unabhängig von der Tatsache, dass sie kopiert wurde, als neues Gerät betrachtet.
- Es wird einer der folgenden Hypervisoren verwendet: VMware™, HyperV oder Xen: der Administrationsagent erkennt die Tatsache des Kopierens der virtuellen Maschine anhand der geänderten ID der virtuellen Hardware.

Die Analyse der Änderungen der virtuellen Hardware ist nicht absolut sicher. Bevor die vorliegende Methode umfassend verwendet wird, muss zuvor ihre Funktionsfähigkeit für die im Unternehmen verwendete Version des Hypervisors auf einer kleinen Anzahl virtueller Maschinen geprüft werden.

Unterstützung des Rollbacks des Dateisystems für Geräte mit Administrationsagent

Kaspersky Security Center ist ein verteiltes Programm. Ein Rollback des Dateisystems auf den vorhergehenden Zustand auf einem der Geräte mit installiertem Administrationsagenten führt zu einer Desynchronisierung der Daten und zur fehlerhaften Ausführung von Kaspersky Security Center.

Ein Rollback des Dateisystems (oder eines Teils davon) auf den vorhergehenden Zustand kann in folgenden Fälle durchgeführt werden:

- Beim Kopieren eines Festplatten-Image.
- Bei der Wiederherstellung des Status der virtuellen Maschine mithilfe der virtuellen Infrastruktur.
- Beim Wiederherstellen der Daten aus der Backup-Kopie oder einem Wiederherstellungspunkt.

Szenarios, in denen Drittanbieter-Programme auf Geräten mit installiertem Administrationsagenten den Ordner "%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\" betreffen, stellen nur für Kaspersky Security Center kritische Szenarios dar. Deshalb ist es erforderlich, diesen Ordner, wenn möglich immer aus der Wiederherstellungsprozedur auszuschließen.

Da in einer Reihe von Unternehmen die Dienstordnung das Ausführen eines Rollbacks des Zustandes des Dateisystems der Geräte voraussetzt, wurde in Kaspersky Security Center ab Version 10 Maintenance Release 1 (Administrationsserver und die Administrationsagenten müssen Versionen 10 Maintenance Release 1 oder höher sein) die Unterstützung der Erkennung eines Rollbacks des Dateisystems auf den Geräten mit installiertem Administrationsagenten hinzugefügt. Im Fall des Erkennens werden solche Geräte automatisch mit einem Administrationsserver mit vollständiger Bereinigung und vollständiger Synchronisierung der Daten verbunden.

In Kaspersky Security Center 15.1 ist die Unterstützung des Erkennens eines Rollbacks des Dateisystems standardmäßig aktiviert.

Falls irgendwie möglich, muss ein Rollback des Ordners %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ auf den Geräten mit installiertem Administrationsagenten vermieden werden, da eine nochmalige vollständige Synchronisierung der Daten einen großen Teil der Ressourcen fordert.

Für das Gerät mit installiertem Administrationsserver ist ein Rollback des Systemzustands unzulässig. Ebenfalls unzulässig ist ein Rollback auf den vorhergehenden Zustand der Datenbank, die vom Administrationsserver verwendet wird.

Der Zustand des Administrationsservers kann nur mithilfe des Standardtools klbackup aus der Backup-Kopie wiederhergestellt werden.

Lokale Installation von Programmen

In diesem Abschnitt wird der Installationsvorgang der Programme beschrieben, die nur lokal auf den Geräten installiert werden können.

Um eine lokale Installation von Programmen auf einem ausgewählten Client-Gerät durchzuführen, müssen Sie über Administratorrechte auf diesem Gerät verfügen.

Gehen Sie wie folgt vor, um Programme auf einem ausgewählten Client-Gerät lokal zu installieren:

1. Installieren Sie auf dem Client-Gerät den Administrationsagenten, und passen Sie die Verbindung des Client-Geräts mit dem Administrationsserver an.
2. Installieren Sie die erforderlichen Programme auf dem Gerät. Folgen Sie dabei den Anweisungen in den Handbüchern zu diesen Programmen.
3. Installieren Sie auf dem Administrator-Arbeitsplatz das Verwaltungs-Plug-in für jedes installierte Programm.

Außerdem unterstützt Kaspersky Security Center die Möglichkeit zur lokalen Installation von Programmen mithilfe eines autonomen Installationspakets. Die Installation aller Kaspersky-Anwendungen wird von Kaspersky Security Center nicht unterstützt.

Lokale Installation des Administrationsagenten

Um den Administrationsagenten lokal auf einem Gerät zu installieren, gehen Sie wie folgt vor:

1. Führen Sie auf dem Gerät die Datei "setup.exe" aus dem Programmpaket aus, das Sie aus dem Internet heruntergeladen haben. Weitere Informationen finden Sie in folgendem Thema: Installationspaket des Administrationsagenten aus dem Programmpaket von Kaspersky Security Center beziehen.

   Ein Fenster wird geöffnet, in dem Sie Kaspersky-Anwendungen zur Installation auswählen können.

2. Starten Sie im Fenster mit der Programmauswahl über den Link **Nur den Kaspersky Security Center Administrationsagenten installieren** den Installationsassistenten des Administrationsagenten. Folgen Sie den Anweisungen des Assistenten.

   a. **Administrationsserver**

      Port

      Gibt den Nicht-SSL-Port an, den der Administrationsserver für das Annehmen der Verbindungen von den Administrationsagenten verwendet.

      Standardmäßig ist diese Option auf 14000 festgelegt.

      SSL-Port

      Gibt den SSL-Port an, den der Administrationsserver für das Annehmen der Verbindungen von den Administrationsagenten verwendet.

      Standardmäßig ist diese Option auf 13000 festgelegt.

      SSL zur Verbindung mit dem Administrationsserver verwenden

      Wenn diese Option aktiviert ist, erfolgt die Verbindung zum Administrationsserver über einen gesicherten Port mit SSL-Protokoll.

      Diese Option ist standardmäßig aktiviert.

      Dem Administrationsagenten erlauben, den UDP-Port zu öffnen

      Wenn diese Option aktiviert ist, öffnet der Installer automatisch den Port, der vom Administrationsserver verwendet wird, um das Client-Gerät zu verwalten und Informationen darüber zu erhalten.

Diese Option ist standardmäßig aktiviert.

UDP-Port

Ermöglicht die Konfiguration des Ports, der vom Administrationsserver verwendet wird, um das Client-Gerät zu verwalten und Informationen darüber zu erhalten.

Standardmäßig ist diese Option auf 15000 festgelegt.

b. **Proxyserver-Konfiguration**

Proxyserver verwenden

Wenn diese Option aktiviert ist, können Sie Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

Diese Option ist standardmäßig deaktiviert.

Adresse

Port

Benutzerkonto

Benutzername des Kontos, unter dessen Namen die Verbindung mit dem Proxy-Server hergestellt wird.

Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

Kennwort

Kennwort des Kontos, unter dessen Namen die Verbindung mit dem Proxy-Server hergestellt wird.

Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

c. **Verbindungs-Gateway**

Verbindungs-Gateway nicht verwenden

Administrationsagent als Verbindungs-Gateway in der DMZ verwenden

Wählen Sie diese Option, um den Administrationsagenten als Verbindungsgateway in der demilitarisierten Zone (DMZ) zu verwenden, um sich mit dem Administrationsserver zu verbinden, mit ihm zu kommunizieren und während der Datenübertragung die Daten auf dem Administrationsagenten sicher aufzubewahren.

Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen

Wählen Sie diese Option und geben Sie anschließend das Gerät an, das als Verbindungs-Gateway fungieren soll.

d. **Zertifikat des Administrationsservers**

e. **Tags des Agenten**

f. **Erweiterte Einstellungen**

Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren

Es wird empfohlen, diese Option aktiviert zu lassen. Sie können diese Option deaktivieren, um die automatischen Updates und Patches für die Komponenten von Kaspersky Security Center zu deaktivieren. Der Administrator kann die automatischen Updates und Patches später mithilfe einer der Richtlinie erneut aktivieren.

Diese Option ist standardmäßig deaktiviert.

Aktivieren Sie den Schutz für den Dienst des Administrationsagenten

Wenn diese Option aktiviert ist, kann nach der Installation des Administrationsagenten auf einem verwalteten Gerät die Komponente nicht ohne die entsprechenden Berechtigungen entfernt oder neu konfiguriert werden. Der Dienst des Administrationsagenten kann nicht beendet werden. Diese Option hat keine Auswirkung auf Domänencontroller.

Aktivieren Sie diese Option, um den Administrationsagenten auf Workstations zu schützen, die mit lokalen Administratorrechten betrieben werden.

Diese Option ist standardmäßig deaktiviert.

Dynamischen Modus für VDI aktivieren

Wenn diese Option aktiviert ist, wird für den auf einer virtuellen Maschine installierten Administrationsagenten der dynamische Modus Virtual Desktop Infrastructure (VDI) aktiviert.

Diese Option ist standardmäßig deaktiviert.

Optimieren Sie die Einstellungen des Administrationsagenten von Kaspersky Security Center für VDI. Deaktivieren Sie die Untersuchung auf Schwachstellen und die Inventarisierung von Programmen und Hardware. Sie können die aktuellen Einstellungen über die Richtlinien des Administrationsagenten bearbeiten.

Wenn diese Option aktiviert ist, sind in den Einstellungen des Administrationsagenten folgende Funktionen deaktiviert:

- Informationen über die installierte Software empfangen
- Informationen über die Hardware empfangen
- Informationen über vorhandene Schwachstellen empfangen
- Informationen über erforderliche Updates empfangen

Diese Option ist standardmäßig deaktiviert.

g. **Programm starten**

Nach Abschluss des Installationsassistenten wird der Administrationsagent auf dem Gerät installiert.

Sie können sich die Eigenschaften des Dienstes des Kaspersky Security Center Administrationsagenten anzeigen lassen, den Administrationsagenten starten und beenden sowie seine Ausführung mit den Standard-Administrationswerkzeugen von Microsoft Windows (Computerverwaltung\Dienste) verfolgen.

Installation des Administrationsagenten im Silent-Modus

Der Administrationsagent kann im Silent-Modus installiert werden, d. h. ohne die interaktive Eingabe von Installationsparametern. Bei der Installation im Silent-Modus wird ein Windows Installer-Paket (msi-Datei) für den Administrationsagenten verwendet. Die msi-Datei befindet sich im Programmpaket für Kaspersky Security Center im Ordner Packages\NetAgent\exec.

Benennen Sie das Installationspaket "Kaspersky Network Agent.msi" nicht um. Ein Umbenennen dieses Pakets kann bei zukünftigen Updates des Administrationsagenten zu Installationsfehlern führen.

Die Installation des Administrationsagenten mittels msi-Paket ist nur im Silent-Modus möglich. Die interaktive Installation mittels msi-Paket wird nicht unterstützt.

Um den Administrationsagenten im Silent-Modus auf einem lokalen Gerät zu installieren:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Verwenden Sie den unten angegebenen Befehl nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.

2. geben Sie folgenden Befehl ein:
   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <Parameters>
   ```
   Dabei steht `Parameter` für eine Liste mit Einstellungen und deren Werten, die durch Leerzeichen getrennt werden (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   In der Liste der Parameter müssen Sie `EULA=1` aufnehmen. Andernfalls wird der Administrationsagent nicht installiert.

Wenn Sie die standardmäßigen Verbindungseinstellungen für Kaspersky Security Center und den Administrationsagenten auf Remote-Geräten verwenden, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` ist der Schlüssel für das Erstellen von Protokollen. Das Protokoll wird im Zuge des Administrationsagenten erstellt und abgespeichert unter C:\windows\temp\nag_inst.log.

Zusätzlich zum Protokoll "ag_inst.log" erstellt das Programm die Datei "$klssinstlib.log", welche das Installationsprotokoll enthält. Die Datei wird in den folgenden Ordnern gespeichert: %windir%\temp oder %temp%. Für etwaige Fehlerbehebungen kann es möglich sein, dass Sie oder ein Spezialist des Technischen Supports von Kaspersky beide Protokolldateien benötigen: "nag_inst.log" und "$klssinstlib.log".

Wenn Sie zusätzlich den Port für die Verbindung zu einem Administrationsserver angeben möchten, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Der Parameter `SERVERPORT` entspricht der Portnummer für die Verbindung zum Administrationsserver.

Die Namen und die möglichen Werte für Einstellungen, die bei der Installation des Administrationsagenten im Silent-Modus verwendet werden können, sind im Abschnitt Installationseinstellungen für den Administrationsagenten angegeben.

Wenn Sie den Administrationsagenten mithilfe von Windows Installer aktualisieren möchten, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Administrationsagent für Linux im Silent-Modus installieren (mit einer Antwort-Datei)

Auf Linux können Sie den Administrationsagenten installieren, indem Sie eine Antwort-Datei verwenden. Dabei handelt es sich im eine Textdatei mit benutzerdefinierten Menge an Installationsparametern: Variablen und ihre entsprechenden Werte. Unter Verwendung der Antwort-Datei können Sie die Installation im Silent-Modus, d. h. ohne Benutzerbeteiligung, ausführen.

Um den Administrationsagent für Linux im Silent-Modus zu installieren:

1. Bereiten Sie das betreffende Linux-Gerät auf die Remote-Installation vor. Laden Sie mithilfe eines passenden Paket-Management-Systems das deb- oder rpm-Paket des Administrationsagenten herunter und erstellen Sie das Remote-Installationspaket.

2. Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

   Wenn Sie den Administrationsagenten auf Geräten mit den Betriebssystemen RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher installieren möchten, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsagent ordnungsgemäß funktioniert.

3. Lesen Sie den Endbenutzer-Lizenzvertrag. Folgen Sie den unten aufgeführten Schritten nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.

4. Erstellen Sie die Antwortdatei (im txt-Format). Fügen Sie der Datei eine Liste mit Variablen im Format "NAME_DER_VARIABLEN=wert_der_variablen" hinzu. Dabei muss jede Variable in einer separaten Zeile angegeben werden.

   Damit die Antwort-Datei korrekt funktioniert, müssen Sie in ihr mindestens diese drei notwendigen Variablen angeben:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Sie können auch weitere Variablen hinzufügen, um spezifischere Parameter für Ihre Remote-Installation zu verwenden. Die folgende Tabelle enthält eine Liste aller Variablen, die in der Antwort-Datei enthalten sein können:

   Für die Installation des Administrationsagenten für Linux im Silent-Modus genutzte Parameter der Antwort-Datei

Für die Installation des Administrationsagenten für Linux im Silent-Modus genutzte Parameter der Antwort-Datei

Name der Variablen	Erforderlich	Beschreibung	Mögliche Werte
KLNAGENT_SERVER	Ja	Beinhaltet den Name des Administrationsservers in Form des voll qualifizierten Domänennamens (FQDN) oder der IP-Adresse.	DNS-Name oder IP-Adresse.
KLNAGENT_AUTOINSTALL	Ja	Gibt an, ob der Silent-Modus für die Installation aktiviert ist.	1—Der Silent-Modus ist aktiviert und der Benutzer erhält während der Installation keinerlei Aufforderungen, etwas zu tun. Andere—Der Silent-Modus ist deaktiviert und der Benutzer kann während der Installation Aufforderungen erhalten, etwas zu tun.
EULA_ACCEPTED	Ja	Gibt an, ob der Benutzer den Endbenutzer-Lizenzvertrag (EULA) des Administrationsagenten akzeptiert hat. Ein Fehlen des Parameters wird als Ablehnung der EULA interpretiert.	1 – Ich bestätige, dass ich die Bestimmungen und Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe und sie verstehe und akzeptiere. Anderer Wert oder keine Angabe – Ich akzeptiere die Bedingungen des Endbenutzer-Lizenzvertrags nicht (die Installation wird nicht ausgeführt).
KLNAGENT_PROXY_USE	Nein	Gibt an, ob die Verbindung zum Administrationsserver Proxy-Einstellungen verwendet. Als Standardwert ist 0 vorgegeben.	1—Die Proxy-Einstellungen werden verwendet. Andere—Die Proxy-Einstellungen werden nicht verwendet.
KLNAGENT_PROXY_ADDR	Nein	Gibt die Adresse des Proxyservers an, der für die Verbindung mit dem Administrationsserver verwendet wird.	DNS-Name oder IP-Adresse.
KLNAGENT_PROXY_LOGIN	Nein	Gibt den Benutzernamen an, der für die Anmeldung am Proxyserver verwendet wird.	Ein beliebiger existierender Benutzername.
KLNAGENT_PROXY_PASSWORD	Nein	Gibt Kennwort des Benutzers an, das für die Anmeldung am Proxyserver verwendet wird.	Ein beliebiger Satz aus alphanumerischen Zeichen, die für das Kennwort-Format des Betriebssystems zulässig sind.
KLNAGENT_VM_VDI	Nein	Gibt an, ob der Administrationsagent auf einem Abbild zur Erstellung dynamischer virtueller Maschinen installiert wird.	1—Der Administrationsagent wird auf einem Abbild installiert, welches anschließend für die Erstellung dynamischer virtueller Maschinen genutzt wird. Andere—Während der Installation wird kein Abbild verwendet.
KLNAGENT_VM_OPTIMIZE	Nein	Gibt an, ob die Administrationsagent-Einstellungen optimal für Hypervisor sind.	1—Die standardmäßigen lokalen Administrationsagent-Einstellungen wurden angepasst, so dass sie eine optimale Verwendung auf Hypervisor erlauben.
KLNAGENT_TAGS	Nein	Liste der Tags, die der Instanz des Administrationsagenten zugewiesen wurden.	Ein oder mehrere Tag-Namen, getrennt durch ein Semikolon.

KLNAGENT_UDP_PORT	Nein	Gibt den vom Administrationsagenten verwendeten UDP-Port an. Als Standardwert ist 15000 vorgegeben.	Eine beliebige existierende Portnummer.
KLNAGENT_PORT	Nein	Gibt den vom Administrationsagenten verwendeten Non-TLS-Port an. Als Standardwert ist 14000 vorgegeben.	Eine beliebige existierende Portnummer.
KLNAGENT_SSLPORT	Nein	Gibt den vom Administrationsagenten verwendeten TLS-Port an. Als Standardwert ist 13000 vorgegeben.	Eine beliebige existierende Portnummer.
KLNAGENT_USESSL	Nein	Gibt an, ob Transport Layer Security (TLS) für die Verbindung verwendet wird.	1 (Standard)—TLS wird verwendet. Andere—TLS wird nicht verwendet.
KLNAGENT_GW_MODE	Nein	Gibt an, ob ein Verbindungsgateway verwendet wird.	1 (Standard)—Die aktuellen Einstellungen wurden nicht geändert (Beim ersten Aufruf ist kein Verbindungsgateway angegeben). 2—Es wird kein Gateway verwendet. 3—Es wird ein Gateway verwendet. KLNAGENT_GW_ADDRESS ist erforderlich. 4—Die Instanz des Administrationsagenten wird als Verbindungsgateway in die demilitarisierte Zone (DMZ) verwendet. Serverzertifikat ist erforderlich.
KLNAGENT_GW_ADDRESS	Nein	Gibt die Adresse des Verbindungsgateways an. Der Wert wird nur ausgewertet, wenn "KLNAGENT_GW_MODE=3" gesetzt ist.	DNS-Name oder IP-Adresse.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Nein	Ermöglicht nach der Installation des Administrationsagenten die Ausführung des Tools zum Registrieren von Benutzern als Gerätebesitzer. Bei deaktivierter Option, steht dem Benutzer die Registrierung als Gerätebesitzer nicht zur Verfügung.	1—Das Tools zum Registrieren von Benutzern als Gerätebesitzer wird nach der Installation des Administrationsagenten ausgeführt. Andere—Deaktiviert.

5. Installieren Sie den Administrationsagenten. Die Umgebungsvariable KLAUTOANSWERS, in welcher der Pfad zur Antwort-Datei angegeben ist, wird an den Installationsbefehl übergeben. Führen Sie einen der folgenden Befehle aus:

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> yum install ./klnagent-<Build-Nummer>.i386.rpm`

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> yum install ./klnagent64-<Build-Nummer>.x86_64.rpm`

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem für die ARM-Architektur zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> yum install ./klnagent64-<Build-Nummer>.aarch64.rpm`

   - Um den Administrationsagenten aus einem DEB-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> apt install ./klnagent_<Build-Nummer>_i386.deb`

   - Um den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> apt install ./klnagent64_<Build-Nummer>_amd64.deb`

   - Um den Administrationsagenten von einem DEB-Paket auf einem 64-Bit-Betriebssystem für die ARM-Architektur zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> apt install ./klnagent64_<Build-Nummer>_arm64.deb`

   Je nach Konfiguration des Betriebssystems können Sie zur Installation des Administrationsagenten auch die Paketmanager rpm, dpkg oder dnf verwenden.

Die Installation des Administrationsagenten für Linux wird im Silent-Modus gestartet und der Benutzer erhält während des Vorgangs keinerlei Aufforderungen, etwas zu tun.

Ein Gerät auf dem Astra Linux im Modus der abgeschlossenen Softwareumgebung ausgeführt wird für die Installation des Administrationsagenten vorbereiten

Vor der Installation des Administrationsagenten auf einem Gerät mit Astra Linux in der abgeschlossenen Softwareumgebung müssen Sie zwei Schritte zur Vorbereitung ausführen: Zum einen den in der folgenden Anleitung beschriebenen und zum anderen den allgemeinen Schritt zur Vorbereitung eines beliebigen Linux-Geräts.

Führen Sie unter einem Benutzerkonto mit Root-Rechten die in dieser Anleitung genannten Befehle aus.

So bereiten Sie Gerät mit Astra Linux im Modus der abgeschlossenen Softwareumgebung für die Installation des Administrationsagenten vor:

1. Öffnen Sie die Datei `/etc/digsig/digsig_initramfs.conf` und geben Sie die folgende Einstellung an:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Führen Sie in der Befehlszeile den folgenden Befehl aus, um das Kompatibilitätspaket zu installieren:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Erstellen Sie ein Verzeichnis für den Anwendungsschlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Legen Sie den Anwendungsschlüssel /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gp in dem Verzeichnis ab, das Sie beim vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Wenn der Programmschlüssel "kaspersky_astra_pub_key.gpg" nicht im Lieferumfang von Kaspersky Security Center enthalten ist, können Sie den Schlüssel über den folgenden Link herunterladen: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Aktualisieren Sie die RAM-Disks:

   ```
   update-initramfs -u -k all
   ```

   Starten Sie das System neu.

Das Linux-Gerät ist bereit für die Installation des Administrationsagenten. Sie können den Administrationsagenten remote, im interaktiven Modus oder im Silent-Modus installieren.

Administrationsagent für Linux im interaktiven Modus installieren

Dieser Artikel beschreibt, wie Sie den Administrationsagenten auf Linux-Geräten im interaktiven Modus installieren. In diesem Modus können Sie die Installationsparameter Schritt für Schritt angeben. Alternativ dazu können Sie eine Antwortdatei verwenden. Dies ist eine Textdatei mit benutzerdefinierten Installationsparametern: Variablen und deren Werte. Unter Verwendung dieser Antwortdatei können Sie die Installation im Silent-Modus ausführen, d. h. ohne Benutzerbeteiligung.

> Wenn Sie den Administrationsagenten auf Geräten mit den Betriebssystemen RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher installieren möchten, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsagent ordnungsgemäß funktioniert.

So installieren Sie den Administrationsagenten im interaktiven Modus:

1. Installieren Sie den Administrationsagenten. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

   - So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem 32-Bit-Betriebssystem:

     ```
     # yum -i klnagent-<Build-Nummer>.i386.rpm
     ```

   - So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem:

     ```
     # yum -i klnagent64-<Build-Nummer>.x86_64.rpm
     ```

- So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem für die Arm-Architektur:

  ```
  # yum -i klnagent64-<Build-Nummer>.aarch64.rpm
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem 32-Bit-Betriebssystem:

  ```
  # apt install ./klnagent_<Build-Nummer>_i386.deb
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem:

  ```
  # apt install ./klnagent64_<Build-Nummer>_amd64.deb
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem für die Arm-Architektur:

  ```
  # apt install ./klnagent64_<Build-Nummer>_arm64.deb
  ```

2. Konfigurieren Sie den Administrationsagenten:

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA). Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung einen der folgenden Werte ein:

   - Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren.
   - Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um den Administrationsagenten zu nutzen, müssen Sie den EULA-Bestimmungen zustimmen.
   - Geben Sie `r` ein, um die EULA erneut anzuzeigen.

4. Geben Sie den DNS-Namen oder die IP-Adresse des Administrationsservers ein.

5. Geben Sie die Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 14000 festgelegt.

6. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

7. Geben Sie `y` ein, wenn Sie für den Datenverkehr zwischen dem Administrationsagenten und dem Administrationsserver die SSL-Verschlüsselung verwenden möchten. Andernfalls geben Sie `n` ein.

8. Wählen Sie eine der folgenden Methoden für die Konfiguration des Administrationsagenten aus:

   - `[1]` – Verbindungs-Gateway nicht konfigurieren.

     Ihr Gerät fungiert nicht als Verbindungs-Gateway und stellt keine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway her.

   - `[2]` – Verbindungs-Gateway nicht verwenden.

     Ihr Gerät stellt keine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway her.

   - `[3]` – Verbindungs-Gateway für die Verbindung mit dem Server verwenden.

     Ihr Gerät stellt eine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway her.

- [4] – Als Verbindungs-Gateway verwenden.

  Ihr Gerät fungiert als Verbindungs-Gateway.

Der Administrationsagent wird auf einem Linux-Gerät installiert.

Lokale Installation des Plug-ins für die Programmverwaltung

Um das Plug-ins für die Programmverwaltung zu installieren,

Starten Sie auf dem Gerät, auf dem die Verwaltungskonsole installiert ist, die ausführbare Datei klcfginst.exe, die zum Programmpaket gehört.

Die Datei klcfginst.exe ist in allen Programmen enthalten, die über Kaspersky Security Center verwaltet werden. Die Installation wird von dem Assistenten begleitet und muss nicht konfiguriert werden.

Programme im Silent-Modus installieren

Um ein Programm im nicht Silent-Modus zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** im Unterordner **Installationspakete** das Installationspaket für das betreffende Programm aus oder erstellen Sie ein neues Installationspaket für dieses Programm.

   Das Installationspaket wird auf dem Administrationsserver im gemeinsamen Ordner im Dienstordner Packages gespeichert. Jedem Installationspaket entspricht dabei der jeweilige Unterordner.

3. Öffnen Sie den Ordner des gewünschten Installationspakets auf eine der folgenden Arten:

   - Kopieren Sie den Ordner, der zum gewünschten Installationspaket passt, vom Administrationsserver auf das Client-Gerät. Öffnen Sie danach den kopierten Ordner auf dem Client-Gerät.
   - Öffnen Sie anschließend vom Client-Gerät aus den gemeinsamen Ordner auf dem Administrationsserver, der zum gewünschten Installationspaket passt.

   Wenn sich der freigegebene Ordner auf einem Gerät befindet, auf dem Microsoft Windows Vista installiert ist, müssen Sie den **Deaktiviert-Wert** für die Benutzerkontensteuerung festlegen: Führen Sie **alle Administratoren im Administratorbestätigungsmodus aus** (**Start** → **Systemsteuerung** → **Verwaltung** → **Lokale Sicherheitsrichtlinie** → **Sicherheitseinstellungen**).

4. Je nach dem gewählten Programm gehen Sie wie folgt vor:

   - Bei Kaspersky Anti-Virus für Windows Workstation, Kaspersky Anti-Virus für Windows Server und Kaspersky Security Center wechseln Sie in den Unterordner exec und starten Sie die ausführbare Datei (mit der Erweiterung .exe) mit dem Parameter /s.
   - Bei den übrigen Kaspersky-Anwendungen starten Sie aus dem geöffneten Ordner die ausführbare Datei (mit der Erweiterung .exe) mit dem Schlüssel /s.

Der Start einer ausführbaren Datei mit den Parametern `EULA=1` und `PRIVACYPOLICY=1` bedeutet, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie vollständig gelesen haben, und sie verstehen und akzeptieren. Außerdem wissen Sie, dass Ihre Daten, wie in der Datenschutzrichtlinie beschrieben, verarbeitet und übertragen werden (einschließlich in Drittländer). Der Text des Lizenzvertrags und der Text der Datenschutzrichtlinie sind im Lieferumfang von Kaspersky Security Center enthalten. Die Annahme der Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie ist die Voraussetzung für die Installation oder das Update des Programms.

Programme mithilfe autonomer Installationspakete installieren

Kaspersky Security Center ermöglicht das Erstellen von autonomen Installationspaketen für Programme. Ein autonomes Installationspaket ist eine ausführbare Datei, die auf einem Webserver abgelegt, per E-Mail verschickt oder auf andere Weise auf ein Client-Gerät übertragen werden kann. Die empfangene Datei kann lokal auf dem Client-Gerät gestartet werden, um das Programm ohne Beteiligung von Kaspersky Security Center zu installieren.

Der eigenständige Administrationsagent für Linux besitzt eine optionale Abhängigkeit vom Tool "nmap". Wenn das nmap-Tool fehlt oder älter als die Version 6.0 ist, wird die Funktion "Broadcast DHCP Discover" nicht unterstützt.

Um ein Programm mithilfe des autonomen Installationspakets zu installieren, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.
3. Wählen Sie im Arbeitsbereich das Installationspaket für das gewünschte Programm aus.
4. Starten Sie den Vorgang zum Erstellen eines autonomen Installationspakets auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf das Installationspaket und wählen Sie **Autonomes Installationspaket erstellen** aus.
   - Klicken Sie mit der rechten Maustaste in den Arbeitsbereich des Installationspaketes und wählen Sie **Autonomes Installationspaket erstellen** aus.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im letzten Schritt des Assistenten eine Methode für die Übertragung des autonomen Installationspakets auf das Client-Gerät aus.
5. Übertragen Sie das autonome Installationspaket für das Programm auf das Client-Gerät.
6. Starten Sie das autonome Installationspaket auf dem Client-Gerät.

   Daraufhin wird das Programm auf dem Client-Gerät mit den Einstellungen installiert, die im autonomen Paket vorgegeben wurden.

Beim Erstellen wird ein autonomes Installationspaket automatisch auf dem Webserver veröffentlicht. Der Link für den Download des autonomen Paketes wird in der Liste der erstellten autonomen Installationspakete angezeigt. Bei Bedarf können Sie die Veröffentlichung des gewählten autonomen Paketes abbrechen und es erneut auf dem Webserver veröffentlichen. Standardmäßig wird für den Download der autonomen Installationspakete Port 8060 verwendet.

Einstellungen des Installationspakets des Administrationsagenten

Um die Einstellungen des Installationspakets des Administrationsagenten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.

   Der Ordner **Remote-Installation** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Klicken Sie mit der rechten Maustaste auf das Installationspaket des Administrationsagenten und wählen Sie **Eigenschaften** aus.

Daraufhin wird das Eigenschaftenfenster des Installationspakets des Administrationsagenten geöffnet.

Allgemein

Der Abschnitt **Allgemein** enthält allgemeine Informationen zum Installationspaket:

- Name des Installationspakets
- Name und Version des Programms, für welches das Installationspaket erstellt wurde
- Größe des Installationspakets
- Erstellungsdatum des Installationspaketes
- Pfad zum Speicherort des Installationspakets

Einstellungen

In diesem Abschnitt können Sie Einstellungen anpassen, die für die Funktionstüchtigkeit des Administrationsagenten sofort nach dessen Installation erforderlich sind. Die Einstellungen in diesem Abschnitt sind nur auf Geräten verfügbar, die unter Windows laufen.

In der Einstellungsgruppe **Zielordner** können Sie einen Ordner auf dem Client-Gerät auswählen, in dem der Administrationsagent installiert werden soll.

- **In Standardordner installieren**

  Bei Auswahl dieser Option wird der Administrationsagent im Ordner <Datenträger>:\Programme\Kaspersky Lab\NetworkAgent installiert. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch erstellt.

  Diese Variante ist standardmäßig ausgewählt.

- **In angegebenen Ordner installieren**

  Bei Auswahl dieser Option wird der Administrationsagent im Ordner installiert, der im Eingabefeld angegeben wurde.

In der Einstellungsgruppe weiter unten können Sie ein Kennwort für die Remote-Deinstallation des Administrationsagenten angeben:

- **Deinstallationskennwort verwenden**

  Wenn die Option aktiviert ist, können Sie nach einem Klick auf **Ändern** das Kennwort für die Deinstallation des Programms angeben (nur für Administrationsagenten auf Geräten unter einem Windows-Betriebssystem verfügbar).

  Diese Option ist standardmäßig deaktiviert.

- **Status**

  Status des Kennworts: **Kennwort gesetzt** oder **Kennwort nicht gesetzt**.

  Standardmäßig ist kein Kennwort gesetzt.

- **Dienst des Administrationsagenten vor unberechtigter Deinstallation und Beendigung schützen sowie Änderung der Einstellungen verhindern**

  Wenn diese Option aktiviert ist, kann nach der Installation des Administrationsagenten auf einem verwalteten Gerät die Komponente nicht ohne die entsprechenden Berechtigungen entfernt oder neu konfiguriert werden. Der Dienst des Administrationsagenten kann nicht beendet werden. Diese Option hat keine Auswirkung auf Domänencontroller.

  Aktivieren Sie diese Option, um den Administrationsagenten auf Workstations zu schützen, die mit lokalen Administratorrechten betrieben werden.

  Diese Option ist standardmäßig deaktiviert.

- **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**

  Wenn diese Option aktiviert ist, werden alle heruntergeladenen Updates und Patches für den Administrationsserver, den Administrationsagenten, die Verwaltungskonsole und iOS MDM-Server automatisch installiert.

  Wenn diese Option deaktiviert ist, werden die heruntergeladenen Updates und Patches nur installiert, sobald Sie deren Status zu *Genehmigt* ändern. Updates und Patches mit dem Status *Nicht festgestellt* werden nicht installiert.

  Diese Option ist standardmäßig aktiviert.

Verbindung

In diesem Abschnitt können Sie die Einstellungen für die Verbindung des Administrationsagenten mit dem Administrationsserver anpassen. Zum Verbindungsaufbau können Sie das SSL- oder UDP-Protokoll verwenden. Geben Sie für die Konfiguration der Verbindung die folgenden Einstellungen an:

- **Administrationsserver**

  Adresse des Geräts, auf dem der Administrationsserver installiert ist.

- **Port**

  Nummer des Ports, über den die Verbindung erfolgt.

- **SSL-Port**

  Nummer des Ports, über den die Verbindung mit dem SSL-Protokoll erfolgt.

- **Zertifikat des Servers verwenden**

  Wenn diese Option aktiviert ist, wird für die Authentifizierung des Zugriffs des Administrationsagenten auf den Administrationsserver eine Zertifikatsdatei verwendet, die über die Schaltfläche **Durchsuchen** angegeben werden kann.

  Wenn diese Option deaktiviert ist, wird die Zertifikatsdatei bei der ersten Verbindung des Administrationsagenten über die Adresse, die im Feld **Serveradresse** angegeben ist, vom Administrationsserver abgerufen.

  Es wird nicht empfohlen, das Kontrollkästchen zu deaktivieren, da das automatische Abrufen des Zertifikats des Administrationsservers durch den Administrationsagenten bei der Verbindung mit dem Server unsicher ist.

  Dieses Kontrollkästchen ist standardmäßig ausgewählt.

- **SSL verwenden**

  Wenn diese Option aktiviert ist, erfolgt die Verbindung zum Administrationsserver über einen gesicherten Port mit SSL-Protokoll.

  Diese Option ist standardmäßig deaktiviert. Wir empfehlen, diese Option nicht zu deaktivieren, damit Ihre Verbindung gesichert bleibt.

- **UDP-Port verwenden**

  Wenn diese Option aktiviert ist, erfolgt die Verbindung zwischen dem Administrationsagenten und dem Administrationsserver über den UDP-Port. Dies ermöglicht es, Client-Geräte zu verwalten und Informationen über sie zu erhalten.

  Der UDP-Port, der auf verwalteten Geräten mit installiertem Administrationsagent geöffnet sein muss. Daher empfehlen wir, diese Option nicht zu deaktivieren.

  Diese Option ist standardmäßig aktiviert.

- **UDP-Port**

  In diesem Feld kann der Port zur Verbindung des Administrationsservers mit dem Administrationsagenten mittels UDP-Protokoll angegeben werden.

  Standardmäßig wird die Nummer des UDP-Ports 15000 verwendet.

- **Ports des Administrationsagenten in der Windows-Firewall öffnen**

  Wenn diese Option aktiviert ist, werden die von Network Agent verwendeten Ports zur Ausschlussliste der Microsoft Windows Firewall hinzugefügt.

  Diese Option ist standardmäßig aktiviert.

- **Proxyserver verwenden**

  Wenn diese Option aktiviert ist, geben Sie die Parameter des Proxyservers an:

  - **Proxyserver-Adresse**
  - **Proxyserver-Port**

  Falls Ihr Proxyserver eine Authentifizierung erfordert, aktivieren Sie die Option **Authentifizierung am Proxyserver** und geben Sie den **Benutzername** und das **Kennwort** für das Konto ein, unter dem die Verbindung mit dem Proxyserver hergestellt wird. Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

Aus Kompatibilitätsgründen wird es nicht empfohlen, die Einstellungen der Proxy-Verbindung in den Einstellungen des Installationspakets für den Administrationsagenten festzulegen.

Erweitert

Im Abschnitt **Erweitert** können Sie konfigurieren, wie das Verbindungs-Gateway verwendet wird. Zu diesem Zweck können Sie Folgendes tun:

- Verwenden Sie den Administrationsagenten als Verbindungsgateway in der demilitarisierten Zone (DMZ), um sich mit dem Administrationsserver zu verbinden, mit ihm zu kommunizieren und während der Datenübertragung die Daten auf dem Administrationsagenten sicher aufzubewahren.
- Verbinden Sie sich unter Verwendung eines Verbindungsgateways mit dem Administrationsserver, um die Anzahl der Verbindungen zum Administrationsserver zu reduzieren. Geben Sie in diesem Fall im Feld **Verbindungs-Gateway-Adresse** die Adresse des Geräts ein, das als Verbindungs-Gateway fungieren soll.
- Konfigurieren Sie die Verbindung für die Virtual Desktop Infrastructure (VDI), wenn Ihr Netzwerk virtuelle Maschinen enthält. Gehen Sie dafür wie folgt vor:
  - **Dynamischen Modus für VDI aktivieren**

    Wenn diese Option aktiviert ist, wird für den auf einer virtuellen Maschine installierten Administrationsagenten der dynamische Modus Virtual Desktop Infrastructure (VDI) aktiviert.

    Diese Option ist standardmäßig deaktiviert.
  - **Einstellungen für VDI optimieren**

    Wenn diese Option aktiviert ist, sind in den Einstellungen des Administrationsagenten folgende Funktionen deaktiviert:
    - Informationen über die installierte Software empfangen
    - Informationen über die Hardware empfangen
    - Informationen über vorhandene Schwachstellen empfangen
    - Informationen über erforderliche Updates empfangen

    Diese Option ist standardmäßig deaktiviert.
- **Ausführen des Tools zur Benutzerregistrierung nach Installation des Administrationsagenten zulassen**

  Wenn diese Option aktiviert ist, wird nach der Installation des Administrationsagenten ein Tool ausgeführt, das den Benutzer als Gerätebesitzer registriert. Diese Option ist standardmäßig deaktiviert.

Zusätzliche Komponenten

In diesem Abschnitt können Sie weitere Komponenten für die gemeinsame Installation mit dem Administrationsagenten auswählen.

Tags

Im Abschnitt **Tags** wird eine Liste mit Schlüsselwörtern (Tags) angezeigt, die Client-Geräten zugewiesen werden können, nachdem der Administrationsagent auf ihnen installiert wurde. Sie können Tags aus der Liste hinzufügen und löschen sowie Tags umbenennen.

Wenn das Kontrollkästchen neben einem Tag aktiviert ist, wird das Tag bei der Installation des Administrationsagenten automatisch zum entsprechenden verwalteten Gerät hinzugefügt.

Ist das Kontrollkästchen neben einem Tag deaktiviert, wird das Tag bei der Installation des Administrationsagenten nicht automatisch zum verwalteten Gerät hinzugefügt. Dieses Tag kann manuell zu Geräten hinzugefügt werden.

Wird ein Tag aus der Liste gelöscht, so wird dieses Tag automatisch auf allen Geräten deaktiviert, zu denen es hinzugefügt wurde.

Revisionsverlauf

In diesem Abschnitt können Sie den Revisionsverlauf des Installationspakets anzeigen. Sie können Revisionen vergleichen, Revisionen ansehen, Revisionen in einer Datei speichern und Beschreibungen von Revisionen hinzufügen und ändern.

Einstellungen für das Installationspaket des Administrationsagenten, die für ein spezifisches Betriebssystem verfügbar sind, werden in der folgenden Tabelle aufgelistet.

Einstellungen des Installationspakets des Administrationsagenten

Abschnitt der Eigenschaft	Windows	Mac	Linux
Allgemein	✓	✓	✓
Einstellungen	✓	—	—
Verbindung	✓	✓ (mit Ausnahme der Optionen **Ports des Administrationsagenten in der Windows-Firewall öffnen** und **Nur automatische Erkennung des Proxyservers verwenden**)	✓ (mit Ausnahme der Optionen **Ports des Administrationsagenten in der Windows-Firewall öffnen** und **Nur automatische Erkennung des Proxyservers verwenden**)
Erweitert	✓	✓	✓
Zusätzliche Komponenten	✓	✓	✓
Tags	✓	✓ (mit Ausnahme der Regeln zur automatischen Zuweisung von Tags)	✓ (mit Ausnahme der Regeln zur automatischen Zuweisung von Tags)
Revisionsverlauf	✓	✓	✓

Anzeigen der Datenschutzrichtlinie

Die Datenschutzrichtlinie ist im Internet unter https://www.kaspersky.com/products-and-services-privacy-policy verfügbar und kann zudem auch Offline angezeigt werden. Sie können die Datenschutzrichtlinie beispielsweise lesen, bevor Sie den Administrationsagenten installieren.

Um die Datenschutzrichtlinie offline zu lesen:

1. Starten Sie den Installer von Kaspersky Security Center.
2. Fahren Sie im Installationsfenster mit dem Link **Installationspakete entpacken** fort.
3. Wählen Sie in der sich öffnenden Liste "Kaspersky Security Center Administrationsagent" aus und klicken Sie anschließend auf **weiter**.

Auf Ihrem Gerät wird im Unterordner "NetAgent" des von Ihnen angegeben Ordners die Datei "privacy_policy.txt" gespeichert.

Bereitstellung der Systeme zur Verwaltung mobiler Geräte

In diesem Abschnitt wird die Bereitstellung der Systeme zur Verwaltung mobiler Geräte mithilfe der Protokolle iOS MDM und Kaspersky Endpoint Security beschrieben.

Bereitstellung des Verwaltungssystems mithilfe des iOS MDM-Protokolls

Kaspersky Security Center ermöglicht Ihnen, mobile Geräte auf der iOS-Plattform zu verwalten. Mobile iOS-Geräte, die mit dem iOS MDM-Server verbunden sind und vom Administrationsserver verwaltet werden, werden als mobile iOS MDM-Geräte bezeichnet.

So werden mobile Geräte mit einem iOS MDM-Server verbunden:

1. Der Administrator installiert den iOS MDM-Server.
2. Der Administrator erhält ein Zertifikat für den Apple Push Notification Service (APNs) ab (Abrufen eines APNs-Zertifikats, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   Ein APNs-Zertifikat ermöglicht dem Administrationsserver eine Verbindung zum APNs-Server aufzubauen, um Push-Benachrichtigungen an iOS MDM-Geräte zu schicken.
3. Der Administrator installiert auf dem iOS MDM-Server das MDM APNs-Zertifikat.
4. Der Administrator erstellt ein iOS MDM-Profil für den Benutzer des mobilen iOS-Geräts.

   Das iOS MDM-Profil enthält eine Auswahl von Einstellungen für die Verbindung von mobilen iOS-Geräten zum Administrationsserver.

Nach der Installation des iOS MDM-Profils und der Synchronisierung mit dem Administrationsserver wird das iOS MDM-Gerät im Unterordner **Mobile Geräte** des Ordners **Verwaltung mobiler Geräte** in der Konsolenstruktur angezeigt.

Installation des iOS MDM-Servers

Um einen iOS MDM-Server auf einem lokalen Gerät zu installieren, gehen Sie wie folgt vor:

1. Starten Sie die ausführbare Datei setup.exe.

   Ein Fenster wird geöffnet, in dem Sie Kaspersky-Anwendungen zur Installation auswählen können.

   Starten Sie im Fenster mit der Programmauswahl über den Link **iOS MDM-Server installieren** den Installationsassistenten für den iOS MDM-Server.
2. Wählen Sie den Zielordner aus.

   Standardmäßig ist es <Laufwerk>:\Programme\Kaspersky Lab\Mobile Device Management for iOS. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch bei der Installation angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** ändern.
3. Geben Sie im Assistentenfenster **Geben Sie die Einstellungen für die Verbindung mit dem iOS MDM-Server an** im Feld **Externer Port zur Verbindung mit dem iOS MDM-Dienst** einen externen Port für die Verbindung von mobilen Geräten mit dem iOS MDM-Dienst an.

Der externe Port 5223 wird durch mobile Geräte für die Verbindung mit dem APNs-Server verwendet. Stellen Sie sicher, dass der Port 5223 in der Firewall für die Verbindung mit dem Adressbereich 17.0.0.0/8 geöffnet ist.

Für die Verbindung des Geräts mit dem iOS MDM-Server wird standardmäßig der Port 443 verwendet. Wenn der Port 443 schon von einem anderen Dienst oder einer anderen App verwendet wird, kann er, beispielsweise, auf den Port 9443 geändert werden.

Der iOS MDM-Server verwendet den externen Port 2197 zum Senden von Benachrichtigungen an den APNs-Server.

Die APNs-Server werden im Modus der ausgeglichenen Auslastung ausgeführt. Die mobilen Geräte verbinden sich nicht immer mit denselben IP-Adressen, um Benachrichtigungen zu erhalten. Der Adressbereich 17.0.0.0/8 ist Apple zugeordnet, daher wird empfohlen, den gesamten Bereich in den Einstellungen der Firewall als erlaubt anzugeben.

4. Wenn Sie die Interaktionsports für die Programmkomponenten manuell anpassen möchten, aktivieren Sie die Option **Lokale Ports manuell anpassen** und nehmen Sie anschließend folgende Einstellungen vor:

   - **Port zur Verbindung mit dem Administrationsagenten**. Geben Sie in diesem Feld den Port für die Verbindung des iOS MDM-Dienstes mit dem Administrationsagenten. Standardmäßig wird Portnummer 9799 verwendet.

   - **Lokaler Port zur Verbindung mit dem iOS MDM-Dienst**. Geben Sie in diesem Feld den lokalen Port für die Verbindung des Administrationsagenten mit dem iOS MDM-Dienst an. Standardmäßig wird Portnummer 9899 verwendet.

   Es wird empfohlen, die Standardeinstellungen zu verwenden.

5. Geben Sie im Fenster **Externe Adresse des Servers für mobile Geräte** des Assistenten im Feld **Webadresse für Remote-Verbindung mit dem Server für mobile Geräte** die Adresse des Client-Geräts an, auf dem der iOS MDM-Server installiert ist.

   Diese Adresse wird für die Verbindung von verwalteten mobilen Geräten zum iOS MDM-Dienst verwendet. Das Client-Gerät muss für eine Verbindung von iOS MDM-Geräten verfügbar sein.

   Sie können die Adresse des Client-Geräts in einem der folgenden Formate angeben:

   - FQDN-Name des Geräts (Beispiel: mdm.example.com)

   - Name des NetBIOS des Geräts

   Bitte fügen Sie das URL-Schema und die Portnummer in die Adresszeile nicht ein. Diese Werte werden automatisch gesetzt.

Der Assistent installiert den iOS MDM-Server auf dem lokalen Gerät. Der iOS MDM-Server wird im Ordner **Verwaltung mobiler Geräte** der Konsolenstruktur angezeigt.

iOS MDM-Server im Silent-Modus installieren

Kaspersky Security Center erlaubt die Installation des iOS MDM-Servers auf dem lokalen Gerät im Silent-Modus. d. h. ohne interaktive Eingabe der Installationseinstellungen.

Um einen iOS MDM-Server auf einem lokalen Gerät im Silent-Modus zu installieren:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Verwenden Sie den unten angegebenen Befehl nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.

2. Führen Sie den folgenden Befehl aus:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <Einstellungsparameter>"
   ```

   wobei `Einstellungsparameter` eine Liste von Einstellungen und deren Werten ist, die durch Leerzeichen voneinander getrennt werden (`PROP1=PROP1VAL PROP2=PROP2VAL`). Die Datei setup.exe befindet sich im Ordner "Server" im Programmpaket von Kaspersky Security Center.

Die Namen und die möglichen Parameterwerte, die bei der Installation des iOS MDM-Servers im Silent-Modus zulässig sind, werden in folgender Tabelle angegeben. Parameter können in beliebiger Reihenfolge angegeben werden.

Parameter für die Installation des iOS MDM-Servers im Silent-Modus

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Endbenutzer-Lizenzvertrags. Dieser Parameter ist obligatorisch.	• 1 – Ich habe die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen, und verstehe und akzeptiere sie. • Anderer Wert oder keine Angabe – die Bedingungen des Endbenutzer-Lizenzvertrags werden abgelehnt (die Installation wird nicht ausgeführt).
DONT_USE_ANSWER_FILE	xml-Datei mit den Installationseinstellungen des iOS MDM-Servers verwenden oder nicht. Die xml-Datei ist Teil des Lieferumfangs des Installationspakets oder befindet sich auf dem Administrationsserver. Der Pfad der Datei muss nicht zusätzlich angegeben werden. Dieser Parameter ist obligatorisch.	• 1 – xml-Datei mit den Parametern nicht verwenden. • Anderer Wert oder keine Werte – xml-Datei mit den Parametern verwenden.
INSTALLDIR	Installationsordner des iOS MDM-Servers. Dieser Parameter ist optional.	String-Wert, z. B. `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Lokaler Port für die Verbindung des iOS MDM-Dienstes mit dem Administrationsagenten. Standardmäßig wird Portnummer 9799 verwendet. Dieser Parameter ist optional.	Zahlenwert.
LOCALSERVERPORT	Lokaler Port für die Verbindung des Administrationsagenten mit dem iOS MDM-Dienst. Standardmäßig wird Portnummer 9899 verwendet. Dieser Parameter ist optional.	Zahlenwert.
EXTERNALSERVERPORT	Port für die Verbindung des Geräts mit dem iOS MDM-Server. Standardmäßig wird Portnummer 443 verwendet. Dieser Parameter ist optional.	Zahlenwert.
EXTERNAL_SERVER_URL	Externe Adresse des Client-Geräts, auf dem der iOS MDM-Server installiert wird. Diese Adresse wird für die Verbindung von verwalteten mobilen Geräten zum iOS MDM-Dienst verwendet. Das Client-Gerät muss für die Verbindung zu iOS MDM verfügbar sein. Die Adresse darf kein URL-Schema und keine Portnummer enthalten, diese Werte werden automatisch hinzugefügt. Dieser Parameter ist optional.	• FQDN-Name des Geräts (Beispiel: mdm.example.com) • Name des NetBIOS des Geräts • IP-Adresse des Geräts

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
WORKFOLDER	Arbeitsordner des iOS MDM-Servers. Wenn kein Arbeitsordner angegeben ist, werden die Daten in den Standardordner geschrieben. Dieser Parameter ist optional.	String-Wert, z. B. `WORKFOLDER=\"C:\work\"`
MTNCY	iOS MDM-Server mit mehreren virtuellen Servern verwenden. Dieser Parameter ist optional.	• 1 – Der iOS MDM-Server wird von mehreren virtuellen Administrationsservern verwendet. • Anderer Wert oder kein Wert – Der iOS MDM-Server wird nicht von mehreren virtuellen Administrationsservern verwendet.

Beispiel:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Die Installationsparameter des iOS MDM-Servers werden in Abschnitt iOS MDM-Server installieren im Detail beschrieben.

Schemata der Bereitstellung eines iOS MDM-Servers

Die Anzahl der installierten Kopien des iOS MDM-Servers kann sowohl ausgehend von der vorhandenen verfügbaren Hardware als auch in Abhängigkeit von der Gesamtmenge der bedienten mobilen Geräte ausgewählt werden.

Dabei muss berücksichtigt werden, dass für eine Installation von Kaspersky Device Management für iOS nicht mehr als 50.000 mobile Geräte empfohlen werden. Zweck Verringerung der Belastung kann die Gesamtheit der Geräte auf mehrere Server mit installiertem iOS MDM-Server verteilt werden.

Die Authentifizierung der iOS MDM-Geräte erfolgt mithilfe der Benutzerzertifikate (das Profil, das auf dem Gerät installiert wird, enthält das Zertifikat des Gerätebesitzers). Daher sind zwei Schemas zur Bereitstellung des iOS MDM-Servers möglich:

- das vereinfachte Schema
- Schema der Bereitstellung unter Verwendung der erzwungenen Delegierung Kerberos (KCD)

Vereinfachtes Schema der Bereitstellung

Bei der Bereitstellung des iOS MDM-Servers gemäß dem vereinfachten Schema werden die mobilen Geräte direkt mit dem Webdienst iOS MDM verbunden. Dabei können für die Authentifizierung der Geräte nur Benutzerzertifikate verwendet werden, die vom Administrationsserver ausgestellt wurden. Die Integration mit Public Key Infrastructure (PKI) ist für Benutzerzertifikate nicht möglich.

Bereitstellungsschema unter Verwendung der erzwungenen Delegierung Kerberos (KCD)

Um das Bereitstellungsschema mit der eingeschränkten Delegierung von Kerberos (KCD) zu verwenden, müssen die folgenden Anforderungen erfüllt sein:

- Der Administrationsserver und der iOS MDM-Server befinden sich im internen Netzwerk der Organisation.
- Es wird ein Reverse-Proxy mit KCD-Unterstützung verwendet.

Dieses Bereitstellungsschema setzt Folgendes voraus:

- Integration in einem Reverse-Proxy, der KCD unterstützt
- Nutzung von KCD zur Authentifizierung mobiler Geräte
- Integration mit der PKI zur Anwendung von Benutzerzertifikaten

Bei Verwendung dieses Bereitstellungsschemas muss Folgendes berücksichtigt werden:

- In der Verwaltungskonsole muss in den Einstellungen des iOS MDM-Webdienstes das Kontrollkästchen **Kompatibilität mit Kerberos Constrained Delegation gewährleisten** aktiviert werden.
- Als Zertifikat des iOS MDM-Webdienstes muss ein benutzerdefiniertes Zertifikat angegeben werden, das definiert wurde, als der iOS MDM-Webdienst auf dem Reverse-Proxy veröffentlicht wurde.
- Die Benutzerzertifikate für die iOS-Geräte müssen vom Domänenzertifizierungszentrum (Certification authority, im Weiteren CA) ausgestellt werden. Wenn es in der Domäne mehrere Stamm-CA gibt, müssen die Benutzerzertifikate von der CA ausgestellt werden, die bei der Veröffentlichung des iOS MDM-Webdienstes auf dem Reverse-Proxy angegeben wurde.

  Die Übereinstimmung des Benutzerzertifikates mit der angegebenen Anforderung kann auf verschiedene Weise gewährleistet werden:

  - Das Benutzerzertifikat im Assistenten für das Erstellen eines iOS MDM-Profils und im Assistenten für die Installation eines Zertifikats angeben.
  - Den Administrationsserver mit Domänen-PKI integrieren und die entsprechende Einstellung in den Regeln für die Ausstellung von Zertifikaten anpassen:

    1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Zertifikate** aus.
    2. Öffnen Sie durch Klicken auf die Schaltfläche **Regeln für das Ausstellen von Zertifikaten anpassen** im Arbeitsbereich des Ordners **Zertifikate** das Fenster **Regeln für das Ausstellen von Zertifikaten**.
    3. Passen Sie im Abschnitt **PKI-Integration** die Integration mit der Public-Key-Infrastruktur an.
    4. Geben Sie im Abschnitt **Mobilgerät-Zertifikat ausstellen** die Quelle der Zertifikate an.

Als Beispiel dienen die Einstellungen für Kerberos Constrained Delegation (KSC) mit den folgenden Annahmen:

- Der Webdienst iOS MDM wird auf Port 443 gestartet
- Der Name des Geräts mit dem Reverse-Proxy lautet "firewall.mydom.local".
- Der Gerätename mit dem iOS MDM-Webdienst lautet iosmdm.mydom.local.
- Der Name der externen Veröffentlichung des Webdienstes iOS MDM lautet iosmdm.mydom.global

Service Principal Name für http/iosmdm.mydom.local

In der Domäne muss der Service Principal Name (SPN) für das Gerät mit dem Webdienst iOS MDM (iosmdm.mydom.local) eingetragen werden:

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Konfigurieren der Domäneneigenschaften des Geräts mit dem Reverse-Proxy (firewall.mydom.local)

Für die Delegierung des Datenverkehres muss das Gerät mit dem Reverse-Proxy (firewall.mydom.local) jenem Dienst vertraut gemacht werden, der gemäß SPN bestimmt wurde (http/iosmdm.mydom.local).

Um das Gerät mit dem Reverse-Proxy dem gemäß SPN bestimmten Dienst vertraut zu machen (http/iosmdm.mydom.local), muss der Administrator wie folgt vorgehen:

1. Im dem Microsoft Management Console-Snap-in namens "Active Directory Users and Computers" muss das Gerät mit installiertem Reverse-Proxy (firewall.mydom.local) ausgewählt werden.

2. In den Eigenschaften des Geräts auf der Registerkarte **Delegation** für den Schalter **Trust this computer for delegation to specified service only**, die Variante **Use any authentication protocol** auswählen.

3. SPN http/iosmdm.mydom.local zur Liste **Services to which this account can present delegated credentials** hinzufügen.

Besonderes (benutzerspezifisches) Zertifikat für den veröffentlichten Webdienst (iosmdm.mydom.global)

Für den Web-Dienst iOS MDM muss ein besonderes (benutzerspezifisches) Zertifikat auf FQDN iosmdm.mydom.global ausgestellt und in der Verwaltungskonsole anstatt des Standardzertifikats in den Einstellungen des Webdienstes iOS MDM angegeben werden.

Es muss berücksichtigt werden, dass im Container mit dem Zertifikat (Datei mit der Erweiterung p12 oder pfx) auch die Kette der Stammzertifikate (öffentlichen Schlüssel) vorhanden sein muss.

Veröffentlichungen des iOS MDM-Webdienstes auf dem Reverse-Proxy

Auf dem Reverse-Proxy muss für den Datenverkehr, der von einem mobilen Gerät auf dem Port 443 von iosmdm.mydom.global eingeht, die KCD auf dem SPN (http/iosmdm.mydom.local) unter Verwendung des für den FQDN (iosmdm.mydom.global) ausgestellten Zertifikats angepasst werden. Dabei muss berücksichtigt werden, dass sowohl bei der Veröffentlichung, als auch beim veröffentlichten Webdienst ein und dasselbe Serverzertifikat verwendet werden muss.

APNs-Zertifikat anfordern

> Wenn Sie bereits über ein APNs-Zertifikat verfügen, ziehen Sie bitte in Erwägung dieses zu erneuern, anstatt ein neues zu erstellen. Wenn Sie das vorhandene APNs-Zertifikat durch ein neu erstelltes ersetzen, verliert der Administrationsserver die Fähigkeit zur Verwaltung der derzeit verbundenen iOS-Mobilgeräte.

Nachdem ein Certificate Signing Request (im Folgenden "CSR-Anfrage" genannt) erstellt wurde, wird beim ersten Schritt des Assistenten zum Anfordern eines APNs-Zertifikats der private Bestandteil des neuen Zertifikats (privater Schlüssel) im Arbeitsspeicher des Geräts gespeichert. Deshalb müssen alle Schritte des Assistenten innerhalb einer einzigen Programmsitzung abgeschlossen werden.

Um ein APNs-Zertifikat anzufordern, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** der Konsolenstruktur den Unterordner **Server für mobile Geräte** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.
3. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des iOS MDM-Servers wird geöffnet.
4. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Zertifikate** aus.
5. Klicken Sie im Abschnitt **Zertifikate** in den Gruppeneinstellungen von **Apple Push Notification-Zertifikat** auf die Schaltfläche **Zertifikat anfordern**.

   Der Assistent zum Anfordern eines APNs-Zertifikats wird gestartet und das Fenster **Zertifikat anfordern** geöffnet.
6. Erstellen Sie einen Certificate Signing Request (im Folgenden "CSR" genannt). Gehen Sie dazu folgendermaßen vor:

   a. Klicken Sie auf **CSR erstellen**.

   b. Machen Sie im folgenden Fenster **CSR erstellen** folgende Angaben: Name der Anfrage, Name des Unternehmens und der Abteilung, Stadt, Bundesland und Land.

   c. Klicken Sie auf **Speichern** und geben Sie den Namen der Datei an, in der die CSR gespeichert werden soll.

   Der private Bestandteil (privater Schlüssel) des zu erstellenden Zertifikats wird im Arbeitsspeicher des Geräts abgelegt.
7. Senden Sie die erstellte Datei über Ihren CompanyAccount mit einer CSR auf Signatur an Kaspersky.

   > Das Signieren Ihrer CSR ist erst möglich, nachdem ein Schlüssel auf das Portal CompanyAccount hochgeladen wurde, der zur Nutzung der Funktionalität "Verwaltung mobiler Geräte" berechtigt.

   Nachdem Ihre Online-Anfrage bearbeitet wurde, erhalten Sie eine von Kaspersky signierte Datei mit der CSR.
8. Senden Sie die signierte Datei mit der CSR an die Webseite von Apple Inc. Verwenden Sie dazu Ihre Apple-ID.

   > Die Verwendung einer persönlichen Apple ID wird nicht empfohlen. Erstellen Sie eine separate Apple-ID für die unternehmensbezogene Verwendung. Ordnen Sie die erstellte Apple-ID nicht dem E-Mail-Postfach eines einzelnen Mitarbeiters, sondern dem Postfach des Unternehmens zu.

   Nachdem die CSR von der Apple Inc. bearbeitet wurde, erhalten Sie den öffentlichen Schlüssel des APNs-Zertifikats. Speichern Sie diese Datei auf der Festplatte.

9. Exportieren Sie das APNs-Zertifikat zusammen mit dem privaten Schlüssel, der beim Erstellen der CSR generiert wurde, in eine PFX-Datei. Gehen Sie wie folgt vor, um dies zu tun:

    a. Klicken Sie im Fenster **Neues APNs-Zertifikat anfordern** auf **CSR abschließen**.

    b. Wählen Sie im folgenden Fenster **Öffnen** die Datei mit dem öffentlichen Schlüssel des Zertifikats aus, die Sie nach der Bearbeitung der CSR von der Apple Inc. erhalten haben, und klicken Sie anschließend auf **Öffnen**.

    Der Export des Zertifikats wird gestartet.

    c. Geben Sie im folgenden Fenster ein Kennwort für den privaten Schlüssel an und klicken Sie auf **OK**.

    Das Kennwort wird für die Installation des APNs-Zertifikats auf dem iOS MDM-Server verwendet.

    d. Geben Sie im Fenster **APNs-Zertifikat speichern** einen Namen für die Datei an, in der das APNs-Zertifikat gespeichert werden soll, wählen einen Ordner zum Speichern der Datei aus, und klicken Sie auf **Speichern**.

Der private und der öffentliche Bestandteil des Zertifikats werden kombiniert. Das APNs-Zertifikat wird in einer PFX-Datei gespeichert. Anschließend kann das erhaltene APNs-Zertifikat auf dem iOS MDM-Server für mobile Geräte installiert werden.

Update des APNs-Zertifikats

Um ein APNs-Zertifikat zu aktualisieren, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** der Konsolenstruktur den Unterordner **Server für mobile Geräte** aus.

2. Wählen Sie im Arbeitsbereich des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.

3. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

    Das Eigenschaftenfenster des iOS MDM-Servers wird geöffnet.

4. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Zertifikate** aus.

5. Im Abschnitt **Zertifikate**, in den Gruppeneinstellungen von **Apple Push Notification-Zertifikat**, klicken Sie auf die Schaltfläche **Aktualisieren**.

    Der Assistent zum Update des APNs-Zertifikats wird gestartet und das Fenster **Update des APNs-Zertifikats** geöffnet.

6. Erstellen Sie einen Certificate Signing Request (im Folgenden "CSR" genannt). Gehen Sie dazu folgendermaßen vor:

    a. Klicken Sie auf **CSR erstellen**.

    b. Machen Sie im folgenden Fenster **CSR erstellen** folgende Angaben: Name der Anfrage, Name des Unternehmens und der Abteilung, Stadt, Bundesland und Land.

    c. Klicken Sie auf **Speichern** und geben Sie den Namen der Datei an, in der die CSR gespeichert werden soll.

    Der private Bestandteil (privater Schlüssel) des zu erstellenden Zertifikats wird im Arbeitsspeicher des Geräts abgelegt.

7. Senden Sie die erstellte Datei über Ihren CompanyAccount mit einer CSR auf Signatur an Kaspersky.

Das Signieren Ihrer CSR ist erst möglich, nachdem ein Schlüssel auf das Portal CompanyAccount hochgeladen wurde, der zur Nutzung der Funktionalität "Verwaltung mobiler Geräte" berechtigt.

Nachdem Ihre Online-Anfrage bearbeitet wurde, erhalten Sie eine von Kaspersky signierte Datei mit der CSR.

8. Senden Sie die signierte Datei mit der CSR an die Webseite von Apple Inc. Verwenden Sie dazu Ihre Apple-ID.

   Die Verwendung einer persönlichen Apple ID wird nicht empfohlen. Erstellen Sie eine separate Apple-ID für die unternehmensbezogene Verwendung. Ordnen Sie die erstellte Apple-ID nicht dem E-Mail-Postfach eines einzelnen Mitarbeiters, sondern dem Postfach des Unternehmens zu.

   Nachdem die CSR von der Apple Inc. bearbeitet wurde, erhalten Sie den öffentlichen Schlüssel des APNs-Zertifikats. Speichern Sie diese Datei auf der Festplatte.

9. Fordern Sie den öffentlichen Schlüssel des Zertifikats an. Gehen Sie dazu folgendermaßen vor:

   a. Wechseln Sie zum Apple Push Certificates Portal. Für die Autorisierung auf dem Portal wird die Apple ID benötigt, die bei der ersten Anforderung des Zertifikats erhalten wurde.

   b. Wählen Sie in der Liste der Zertifikate das Zertifikat, dessen APSP-Name (ein Name im Format "APSP: <Nummer>") mit dem APSP-Namen des Zertifikats übereinstimmt, das vom iOS MDM-Server verwendet wird, und klicken Sie auf die Schaltfläche **Aktualisieren**.

      Das APNs-Zertifikat wird aktualisiert.

   c. Speichern Sie das vom Portal erstellte Zertifikat.

10. Exportieren Sie das APNs-Zertifikat zusammen mit dem privaten Schlüssel, der beim Erstellen der CSR generiert wurde, in eine PFX-Datei. Gehen Sie dazu folgendermaßen vor:

    a. Klicken Sie im Fenster **Update des APNs-Zertifikats** auf **CSR abschließen**.

    b. Wählen Sie im folgenden Fenster **Öffnen** die Datei mit dem öffentlichen Schlüssel des Zertifikats aus, die Sie nach der Bearbeitung der CSR von der Apple Inc. erhalten haben, und klicken Sie auf **Öffnen**.

       Der Export des Zertifikats wird gestartet.

    c. Geben Sie im folgenden Fenster ein Kennwort für den privaten Schlüssel an und klicken Sie auf **OK**.

       Das Kennwort wird für die Installation des APNs-Zertifikats auf dem iOS MDM-Server verwendet.

    d. Geben Sie im folgenden Fenster **Update des APNs-Zertifikats** einen Namen für die Datei an, in der das APNs-Zertifikat gespeichert werden soll, wählen einen Ordner zum Speichern der Datei aus, und klicken Sie auf **Speichern**.

Der private und der öffentliche Bestandteil des Zertifikats werden kombiniert. Das APNs-Zertifikat wird in einer PFX-Datei gespeichert.

Das Reservezertifikat des iOS MDM-Servers konfigurieren

Mit der iOS MDM-Server-Funktionalität können Sie ein Reservezertifikat ausstellen. Dieses Zertifikat ist zur Verwendung in iOS MDM-Profilen vorgesehen, um nach Ablauf des iOS MDM-Server-Zertifikats einen nahtlosen Wechsel verwalteter iOS-Geräte sicherzustellen.

Wenn Ihr iOS MDM-Server ein von Kaspersky ausgestelltes Standardzertifikat verwendet, können Sie ein Reservezertifikat ausstellen (oder Ihr eigenes benutzerdefiniertes Zertifikat als Reserve angeben), bevor das iOS MDM-Server-Zertifikat abläuft. Standardmäßig wird das Reservezertifikat automatisch 60 Tage vor Ablauf des iOS MDM-Server-Zertifikats ausgestellt. Das Reservezertifikat des iOS MDM-Server wird sofort nach Ablauf des iOS MDM-Server-Zertifikats zum Hauptzertifikat. Der öffentliche Schlüssel wird über Konfigurationsprofile an alle verwalteten Geräte verteilt, sodass Sie ihn nicht manuell übertragen müssen.

Um das Reservezertifikat eines iOS MDM-Servers auszustellen oder ein benutzerdefiniertes Reservezertifikat anzugeben:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Verwaltung mobiler Geräte** den Unterordner **Server für mobile Geräte**.

2. Wählen Sie in der Liste "Server für mobile Geräte" den entsprechenden iOS MDM-Server aus und klicken Sie im rechten Bereich auf **Einstellungen des iOS MDM-Servers konfigurieren**.

3. Wählen Sie im angezeigten Einstellungsfenster des iOS MDM-Servers den Abschnitt **Zertifikate** aus.

4. Führen Sie im Einstellungsblock **Reservezertifikat** eine der folgenden Aktionen aus:

   - Wenn Sie weiterhin ein selbstsigniertes Zertifikat verwenden möchten (d. h. das von Kaspersky ausgestellte):

     a. Klicken Sie auf die Schaltfläche **Ausstellen**.

     b. Wählen Sie im folgenden Fenster **Aktivierungsdatum** eine der beiden Optionen für das Datum aus, an dem das Reservezertifikat angewendet werden muss:

        - Wenn Sie das Reservezertifikat anwenden möchten, sobald das aktuelle Zertifikat abläuft, wählen Sie die Option **Nach Ablauf des aktuellen Zertifikats**.

        - Wenn Sie das Reservezertifikat anwenden möchten, bevor das aktuelle Zertifikat abläuft, wählen Sie die Option **Nach einem bestimmten Zeitraum (Tage)**. Geben Sie im Eingabefeld neben dieser Option den Zeitraum an, nach dem das aktuelle Zertifikat durch das Reservezertifikat ersetzt werden muss.

     > Die Gültigkeitsdauer des von Ihnen angegebenen Reservezertifikats darf die Gültigkeitsdauer des aktuellen iOS MDM-Server-Zertifikats nicht überschreiten.

     c. Klicken Sie auf die Schaltfläche **OK**.

     Das Reservezertifikat des iOS MDM-Servers wird ausgestellt.

   - Wenn Sie ein von Ihrer Zertifizierungsstelle ausgestelltes benutzerdefiniertes Zertifikat verwenden möchten:

     a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

     b. Geben Sie im angezeigten Windows-Datei-Explorer eine Zertifikatsdatei im pem-, pfx- oder p12-Format an, die auf Ihrem Gerät gespeichert ist, und klicken Sie dann auf **Öffnen**.

     Ihr benutzerdefiniertes Zertifikat wird als Reservezertifikat des iOS MDM-Servers angegeben.

Sie haben das Reservezertifikat für einen iOS MDM-Server angegeben. Die Details des Reservezertifikats werden im Einstellungsblock **Reservezertifikat** angezeigt (Zertifikatname, Ausstellername, Ablaufdatum und ggf. das Datum, an dem das Reservezertifikat angewendet werden muss).

APNs-Zertifikat auf dem iOS MDM-Server installieren

Anschließend muss das APNs-Zertifikat auf dem iOS MDM-Server installiert werden.

Um ein APNs-Zertifikat auf dem iOS MDM-Server zu installieren, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** der Konsolenstruktur den Unterordner **Server für mobile Geräte** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.
3. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des iOS MDM-Servers wird geöffnet.
4. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Zertifikate** aus.
5. Klicken Sie im Abschnitt **Zertifikate** im Einstellungsbereich **Apple Push Notification-Zertifikat** auf die Schaltfläche **Installieren**.
6. Wählen Sie die PFX-Datei aus, die das APNs-Zertifikat enthält.
7. Geben Sie das Kennwort des privaten Schlüssels an, das beim Export des APNs-Zertifikats festgelegt wurde.

Das APNs-Zertifikat wird auf dem iOS MDM-Server installiert. Informationen über das Zertifikat werden im Eigenschaftenfenster des iOS MDM-Servers unter **Zertifikate** angezeigt.

Einstellungen für den Zugriff auf den Dienst Apple Push Notification

Für die ordnungsgemäße Ausführung des Webdienstes iOS MDM sowie für die Gewährleistung einer rechtzeitigen Reaktion der mobilen Geräte auf die Befehle des Administrators muss in den Einstellungen des iOS MDM-Servers das Zertifikat Apple Push Notification Service (im Weiteren APNs-Zertifikat) angegeben werden.

Zusammen mit dem Dienst Apple Push Notification (im Weiteren APNs) stellt der Webdienst iOS MDM über den Port 2197 (ausgehend) eine Verbindung mit der externen Adresse api.push.apple.com her. Deshalb muss der Webdienst iOS MDM für den Adressbereich 17.0.0.0/8 Zugriff auf den Port TCP 2197 gewähren. Von Seiten der iOS-Geräte – Zugriff auf den Port TCP 5223 für den Adressbereich 17.0.0.0/8.

Wenn der Zugriff auf APNs von Seiten des Webdienstes iOS MDM über einen Proxyserver erfolgt, muss auf dem Gerät mit installierten Webdienst iOS MDM wie folgt vorgegangen werden:

1. Folgende Zeilen in die Registrierung eintragen:

   - Für 32-Bit-Betriebssysteme:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

   - Für 64-Bit-Betriebssysteme:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

2. Dienst des Webdienstes iOS MDM neu starten.

Allgemeines Zertifikat ausstellen und auf dem mobilen Gerät installieren

Um ein allgemeines Zertifikat für den Benutzer auszustellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** ein Benutzerkonto aus.
2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Zertifikat installieren** aus.

   Der Assistent für die Installation eines Zertifikats wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird ein Zertifikat erstellt und zur Liste der Benutzerzertifikate hinzugefügt.

Der Benutzer lädt das ausgestellte Zertifikat gemeinsam mit dem Installationspaket herunter, in dem sich das iOS MDM-Profil befindet.

Nachdem das mobile Gerät mit dem iOS MDM-Server verbunden wurde, werden auf dem Benutzergerät die Einstellungen des iOS MDM-Profils angewendet. Der Administrator kann verbundene Geräte verwalten.

Das mobile Gerät des Benutzers, das mit dem iOS MDM-Server verbunden ist, wird im Unterordner **Mobile Geräte** angezeigt, der sich im Ordner **Verwaltung mobiler Geräte** der Konsolenstruktur befindet.

KES-Gerät zur Liste der verwalteten Geräte hinzufügen

Um ein KES-Gerät des Benutzers mithilfe eines Links zu Google Play™ zur Liste der verwalteten Geräte hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** aus.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Wählen Sie das Benutzerkonto, dessen mobiles Gerät Sie zur Liste der verwalteten Geräte hinzufügen möchten.

3. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Mobiles Gerät hinzufügen** aus.

   Der Assistent für die Verbindung eines mobilen Gerätes wird gestartet. Im Fenster **Quelle des Zertifikats** des Assistenten muss die Methode zur Erstellung des allgemeinen Zertifikats angegeben werden, mit dessen Hilfe der Administrationsserver das mobile Gerät identifiziert. Sie können ein allgemeines Zertifikat auf eine von zwei Arten angeben:

   - Automatisch ein allgemeines Zertifikat mithilfe des Administrationsservers erstellen und das Zertifikat auf dem Gerät hinzufügen
   - Die Datei des allgemeinen Zertifikats angeben

4. Wählen Sie im Fenster **Gerätetyp** des Assistenten die Variante **Link zu Google Play**.

5. Konfigurieren Sie im Fenster **Benachrichtigungsmethode** des Assistenten die Benachrichtigungseinstellungen für den Benutzer des mobilen Geräts für die Benachrichtigung über die Erstellung eines Zertifikats (mithilfe einer SMS-Nachricht, per E-Mail oder durch Anzeige der Information nach Beendigung des Assistenten).

6. Klicken Sie im Fenster "Informationen zum Zertifikat" auf die Schaltfläche **Fertig**, um den Assistenten zu beenden.

Daraufhin werden ein Link und ein QR-Code zum Herunterladen von Kaspersky Endpoint Security für Android von Google Play an das Gerät des Benutzers gesendet. Der Benutzer wechselt mithilfe des Links oder durch Scannen des QR-Codes zum App Store Google Play. Daraufhin zeigt das Betriebssystem dem Benutzer eine Zustimmungsaufforderung zur Installation von Kaspersky Endpoint Security für Android an. Nach dem Herunterladen und der Installation von Kaspersky Endpoint Security für Android stellt das mobile Gerät eine Verbindung zum Administrationsserver her und lädt das allgemeine Zertifikat herunter. Nach der Installation des Zertifikats auf dem mobilen Gerät wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Verwaltung mobiler Geräte** der Konsolenstruktur angezeigt.

Wenn die App Kaspersky Endpoint Security für Android bereits auf dem Gerät installiert ist, muss der Benutzer die vom Administrator erhaltenen Verbindungseinstellungen für den Administrationsserver selbstständig eingeben. Nach der Konfiguration der Verbindungseinstellungen stellt das mobile Gerät eine Verbindung mit dem Administrationsserver her. Der Administrator stellt ein allgemeines Zertifikat für das Gerät aus und sendet dem Benutzer eine E-Mail-Nachricht oder eine SMS mit dem Benutzernamen und dem Kennwort zum Herunterladen des Zertifikats. Der Benutzer lädt das allgemeine Zertifikat herunter und installiert es auf seinem Gerät. Nach der Installation des Zertifikats auf dem mobilen Gerät wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Verwaltung mobiler Geräte** der Konsolenstruktur angezeigt. In diesem Fall wird Kaspersky Endpoint Security für Android nicht nochmals heruntergeladen und installiert.

Verbindung von KES-Geräten mit dem Administrationsserver

Abhängig von der Verbindungsmethode der Geräte mit dem Administrationsserver existieren zwei Bereitstellungsschemas von Kaspersky Device Management für iOS für KES-Geräte:

- Bereitstellungsschema unter Verwendung einer direkten Verbindung der Geräte mit dem Administrationsserver
- Schema für die Bereitstellung mit einem Reverse-Proxy, der die eingeschränkte Delegierung von Kerberos unterstützt

Direkte Verbindung der Geräte mit dem Administrationsserver

KES-Geräte können direkt mit dem Port 13292 des Administrationsservers verbunden werden.

Abhängig von der Art der Authentifizierung existieren zwei Varianten zur Verbindung von KES-Geräten mit dem Administrationsserver:

- Verbindung der Geräte unter Verwendung eines Benutzerzertifikats
- Verbindung der Geräte ohne Benutzerzertifikat

Verbindung eines Geräts unter Verbindung eines Benutzerzertifikats

Bei der Verbindung eines Geräts unter Verwendung eines Benutzerzertifikats erfolgt ein Anbinden des Geräts an das Benutzerkonto, dem mithilfe des Administrationsservers ein entsprechendes Zertifikat zugewiesen wurde.

Es wird in diesem Fall die beidseitige SSL-Authentifizierung SSL (two-way SSL authentication, mutual authentication) verwendet. Sowohl der Administrationsserver als auch das Gerät werden mithilfe der Zertifikate authentifiziert.

Verbindung des Geräts ohne Benutzerzertifikat

Bei der Verbindung des Geräts ohne Benutzerzertifikat wird es nicht an ein Benutzerkonto auf dem Administrationsserver angebunden. Ruft das Gerät jedoch ein beliebiges Zertifikat ab, erfolgt ein Anbinden des Geräts an den Benutzer, dem das entsprechende Zertifikat mithilfe des Administrationsservers zugewiesen wurde.

Bei der Verbindung des Geräts mit dem Administrationsserver wird die einseitige SSL-Authentifizierung (one-way SSL authentication) verwendet, bei der nur der Administrationsserver mithilfe des Zertifikates authentifiziert wird. Nachdem das Gerät ein Benutzerzertifikat abgerufen hat, wird der Authentifizierungstyp auf beidseitige SSL-Authentifizierung (2-way SSL authentication, mutual authentication) geändert.

Anschlussschema für KES-Geräte mit dem Server unter Verwendung der erzwungenen Delegierung Kerberos (KCD)

Das Verbindungsschema für KES-Geräte zum Administrationsserver unter Verwendung von Kerberos Constrained Delegation (KCD) setzt voraus:

- Integration mit einem Reverse-Proxy, der KCD unterstützt.
- Nutzung von Kerberos Constrained Delegation (im Weiteren "KCD") zur Authentifizierung mobiler Geräte.
- Integration mit der Infrastruktur der offenen Schlüssel (Public Key Infrastructure, im Weiteren PKI) zur Verwendung von Benutzerzertifikaten.

Bei Verwendung dieses Verbindungsschemas muss Folgendes berücksichtigt werden:

- Der Verbindungstyp der KES-Geräte zum Reverse-Proxy muss "Zwei-Wege-SSL-Authentifizierung" sein. Das heißt, das Gerät muss gemäß seines proprietären Benutzerzertifikats mit dem Reverse-Proxy verbunden werden. Dazu muss im Installationspaket von Kaspersky Endpoint Security für Android, das auf dem Gerät installiert ist, das Benutzerzertifikat integriert sein. Dieses KES-Paket muss vom Administrationsserver speziell für das betreffende Gerät (den Benutzer) erstellt worden sein.
- Anstelle des Standardserverzertifikats muss für das mobile Protokoll ein besonderes (benutzerspezifisches) Zertifikat angegeben werden:

  1. Aktivieren Sie Im Eigenschaftenfenster des Administrationsservers im Abschnitt **Einstellungen** das Kontrollkästchen **Port für mobile Geräte öffnen**, wählen Sie in der Dropdown-Liste die Option **Zertifikat hinzufügen** aus.
  2. Geben Sie im folgenden Fenster dasselbe Zertifikat an, das auf dem Reverse-Proxy bei der Veröffentlichung des Zugriffspunkts für das mobile Protokoll auf dem Administrationsserver festgelegt wurde.

- Die Benutzerzertifikate für die KES-Geräte müssen von der Domänen-Certificate Authority (CA) ausgestellt werden. Beachten Sie dabei: Sollte die Domain mehrere Stamm-CAs beinhalten, müssen die Benutzerzertifikate mit jener CA ausgestellt werden, die bei der Veröffentlichung auf dem Reverse-proxy festgelegt wurde.

  Die Übereinstimmung mit den Anforderungen des oben erwähnten Benutzerzertifikates kann auf verschiedene Weisen gewährleistet werden:

  - Ein besonderes Benutzerzertifikat im Assistenten für das Erstellen von Installationspaketen und im Assistenten für die Installation eines Zertifikats angeben.
  - Den Administrationsserver mit Domänen-PKI integrieren und die entsprechende Einstellung in den Regeln für die Ausstellung von Zertifikaten anpassen:

    1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Zertifikate** aus.
    2. Öffnen Sie durch Klicken auf die Schaltfläche **Regeln für das Ausstellen von Zertifikaten anpassen** im Arbeitsbereich des Ordners **Zertifikate** das Fenster **Regeln für das Ausstellen von Zertifikaten**.
    3. Passen Sie im Abschnitt **PKI-Integration** die Integration mit der Public-Key-Infrastruktur an.
    4. Geben Sie im Abschnitt **Mobilgerät-Zertifikat ausstellen** die Quelle der Zertifikate an.

Als Beispiel dienen die Einstellungen für die eingeschränkte Delegierung von KCD mit den folgenden Annahmen:

- Der Zugriffspunkt auf das mobile Protokoll auf dem Administrationsserver liegt auf Port 13292.
- Der Name des Geräts mit dem Reverse-Proxy lautet "firewall.mydom.local".
- Der Gerätename mit dem Administrationsserver lautet ksc.mydom.local.
- Der Name der externen Veröffentlichung des Zugriffspunkts auf das mobile Protokoll lautet kes4mob.mydom.global.

Domänenbenutzerkonto für den Administrationsserver

Das Domänenbenutzerkonto (beispielsweise KSCMobileSrvcUsr), unter dem der Dienst des Administrationsservers ausgeführt werden soll, muss erstellt werden. Das Benutzerkonto für den Dienst des Administrationsservers kann bei der Installation des Administrationsservers oder mithilfe des Tools klsrvswch angegeben werden. Das Tool klsrvswch befindet sich im Installationsordner des Administrationsservers. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

Das Domänenbenutzerkonto muss aus folgenden Gründen angegeben werden:

- Die Funktionalität zur Verwaltung von KES-Geräten ist ein untrennbarer Bestandteil des Administrationsservers.
- Für die ordnungsgemäße Ausführung von Kerberos Constrained Delegation (KCD) muss die Empfängerseite (d. h. der Administrationsserver) unter einem Domänenbenutzerkonto ausgeführt werden.

Service Principal Name für http/kes4mob.mydom.local

In der Domäne unter dem Benutzerkonto KSCMobileSrvcUsr ist es erforderlich, den Service Principal Name (SPN) für die Veröffentlichung des Dienstes des mobilen Protokolls auf Port 13292 des Geräts mit dem Administrationsserver zu registrieren. Für das Gerät kes4mob.mydom.local mit dem Administrationsserver sieht dies folgendermaßen aus:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Konfigurieren der Domäneneigenschaften des Geräts mit dem Reverse-Proxy (firewall.mydom.local)

Für die Delegierung des Datenverkehres muss das Gerät mit dem Reverse-Proxy (firewall.mydom.local) jenem Dienst vertraut gemacht werden, der gemäß SPN festgelegt wurde (http/kes4mob.mydom.local:13292).

Um das Gerät mit dem Reverse-Proxy dem gemäß SPN bestimmten Dienst vertraut zu machen (http/kes4mob.mydom.local:13292), muss der Administrator wie folgt vorgehen:

1. Im dem Microsoft Management Console-Snap-in namens "Active Directory Users and Computers" muss das Gerät mit installiertem Reverse-Proxy (firewall.mydom.local) ausgewählt werden.
2. In den Eigenschaften des Geräts auf der Registerkarte **Delegation** für den Schalter **Trust this computer for delegation to specified service only**, die Variante **Use any authentication protocol** auswählen.
3. SPN http/kes4mob.mydom.local:13292 zur Liste **Services to which this account can present delegated credentials** hinzufügen.

Besonderes (benutzerspezifisches) Zertifikat für die Veröffentlichung (kes4mob.mydom.global)

Für die Veröffentlichung des mobilen Protokolls des Administrationsservers ist es erforderlich, ein besonderes (benutzerspezifisches) Zertifikat auf FQDN kes4mob.mydom.global auszustellen und es in der Verwaltungskonsole anstatt des Standardserverzertifikats in den Einstellungen des mobilen Protokolls des Administrationsservers anzugeben. Dazu muss im Eigenschaftenfenster des Administrationsservers im Abschnitt **Einstellungen** das Kontrollkästchen **Port für mobile Geräte öffnen** aktiviert und in der Dropdown-Liste die Option **Zertifikat hinzufügen** ausgewählt werden.

Es muss berücksichtigt werden, dass im Container mit dem Serverzertifikat (Datei mit der Erweiterung p12 oder pfx) auch die Kette der Stammzertifikate (öffentlichen Schlüssel) vorhanden sein muss.

Veröffentlichung auf dem Reverse-Proxy konfigurieren

Auf dem Reverse-Proxy muss für den Datenverkehr, der ausgehend von einem mobilen Gerät auf dem Port 139292 von kes4mob.mydom.global eingeht, die KCD auf dem SPN (http/kes4mob.mydom.local.13292) unter Verwendung des für den FQDN (kes4mob.mydom.global ausgestellten Zertifikats angepasst werden. Dabei muss berücksichtigt werden, dass sowohl bei der Veröffentlichung, als auch beim veröffentlichten Zugriffspunkt (Port 13292 des Administrationsservers) ein und dasselbe Serverzertifikat verwendet werden muss.

Verwendung von Firebase Cloud Messaging

Zur rechtzeitigen Zustellung von Befehlen auf KES-Geräten die durch das Android-Betriebssystem verwaltet werden, wird in Kaspersky Security Center das System der Push-Benachrichtigung verwendet. Push-Benachrichtigungen zwischen KES-Geräten und dem Administrationsserver werden mittels Firebase Cloud Messaging (im Folgenden als FCM bezeichnet) ausgetauscht. In der Kaspersky Security Center Verwaltungskonsole können Sie die Einstellungen für Firebase Cloud Messaging festlegen, um KES-Geräte an den Dienst anzuschließen.

Um die Einstellungen für Firebase Cloud Messaging zu erhalten, müssen Sie über ein Google-Benutzerkonto verfügen.

So aktivieren die Verwendung von FCM:

1. Wählen Sie in der Verwaltungskonsole zuerst den Knoten **Verwaltung mobiler Geräte** aus und dann den Ordner **Mobile Geräte**.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Mobile Geräte**, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie im Ordnereinstellungen den Abschnitt **Einstellungen von Firebase Cloud Messaging**.
4. Geben Sie im Feld **Firebase-Projektnummer** die ID des FCM Sender ein.
5. Wählen Sie im Feld **Datei mit privatem Schlüssel (JSON-Format)** die Datei mit dem privaten Schlüssel aus.

Bei der nächsten Synchronisierung mit dem Administrationsserver werden KES-Geräte, die durch das Android-Betriebssystem verwaltet werden, an den Dienst Firebase Cloud Messaging angeschlossen.

Sie können die Einstellungen für Firebase Cloud Messaging mithilfe der Schaltfläche **Einstellungen zurücksetzen** ändern.

Wenn Sie zu einem anderen Firebase-Projekt wechseln, müssen Sie 10 Minuten warten, bis FCM fortgesetzt wird.

Der Dienst FCM arbeitet in den folgenden Adressbereichen:

- Seitens des KES-Gerätes ist der Zugriff auf die Ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) der folgenden Adressen erforderlich:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Alle IP-Adressen aus der Liste "Google ASN 15169"
- Seitens des Administrationsservers ist der Zugriff auf den Port 443 (HTTPS) der folgenden Adressen erforderlich:
  - fcm.googleapis.com
  - Oder auf allen IP aus der Liste "Google ASN 15169"

Falls in der Verwaltungskonsole in den Eigenschaften des Administrationsservers die Proxyserver-Einstellungen (**Erweitert** / **Einstellungen für den Internetzugriff konfigurieren**) festgelegt sind, werden sie für die Interaktion mit FCM verwendet.

Konfiguration von FCM: Datei mit der Sender ID und dem privaten Schlüssel abrufen

So konfigurieren Sie FCM:

1. Registrieren Sie sich auf dem Google-Portal.
2. Gehen Sie zur Firebase-Konsole.
3. Führen Sie eine der folgenden Aktionen aus:
   - Erstellen Sie ein neues Projekt, indem Sie auf **Projekt erstellen** klicken und den Anweisungen auf dem Bildschirm folgen.
   - Öffnen Sie ein vorhandenes Projekt.
4. Klicken Sie auf das Zahnrad-Symbol und wählen Sie **Projekteinstellungen** aus.

   Das Fenster **Projekteinstellungen** wird geöffnet.
5. Wählen Sie die Registerkarte **Cloud Messaging** aus.
6. Rufen Sie die relevante Sender-ID aus dem Feld **Sender ID** im Abschnitt **Firebase Cloud Messaging API (V1)** ab.

7. Wählen Sie die Registerkarte **Dienstkonten** aus und klicken Sie auf **Neuen privaten Schlüssel generieren**.

8. Klicken Sie im neuen Fenster auf **Schlüssel generieren**, um eine Datei mit einem privaten Schlüssel zu generieren und herunterzuladen.

Firebase Cloud Messaging ist jetzt konfiguriert.

Integration mit Public Key Infrastructure

Die Integration mit der Infrastruktur der offenen Schlüssel (Public Key Infrastructure, im Weiteren PKI) dient in erster Linie zur Vereinfachung der Ausstellung von Domänenbenutzerzertifikaten durch den Administrationsserver.

Der Administrator kann dem Benutzer in der Verwaltungskonsole ein Domänenzertifikat zuweisen. Dies kann auf eine der folgenden Weisen erfolgen:

- Dem Benutzer ein besonderes (benutzerspezifisches) Zertifikat aus der Datei im Assistenten für die Verbindung eines neuen Geräts oder im Assistenten für die Installation eines Zertifikats zuweisen.

- Eine Integration mit PKI ausführen und PKI als Quelle der Zertifikate für den konkreten Zertifikatstyp oder für alle Zertifikatstypen festlegen.

Die Einstellungen für die PKI-Integration werden im Arbeitsbereich des Ordners **Verwaltung mobiler Geräte** / **Zertifikate** verfügbar, indem Sie den Link **In Public-Key-Infrastruktur integrieren** anklicken.

Grundprinzip der PKI-Integration für die Ausstellung von Benutzerzertifikaten für Domänen

In der Verwaltungskonsole muss über den Link **In Public-Key-Infrastruktur integrieren** im Arbeitsbereich des Ordners **Verwaltung mobiler Geräte/Zertifikate** das Domänenbenutzerkonto festgelegt werden, das vom Administrationsserver für die Ausstellung von Domänenbenutzerzertifikaten mittels Domänen-CA verwendet wird (in Weiteren das Benutzerkonto, unter dem die PKI-Integration ausgeführt wird).

Dabei ist muss Folgendes berücksichtigt werden:

- In den Einstellungen der PKI-Integration gibt es die Möglichkeit, eine Standardvorlage für alle Zertifikatstypen anzugeben. In den Regeln für das Ausstellen von Zertifikaten (die Regeln sind im Arbeitsbereich des Ordners **Verwaltung mobiler Geräte/Zertifikate** mithilfe der Schaltfläche **Regeln für das Ausstellen von Zertifikaten anpassen** verfügbar) besteht hingegen die Möglichkeit, die Vorlage für jeden Typ des Zertifikates separat festzulegen.

- Auf dem Gerät mit dem installierten Administrationsserver muss im Zertifikatsspeicher des Benutzerkontos, unter dem die PKI-Integration ausgeführt wird, das Spezialzertifikat Enrollment Agent (EA) installiert sein. Das Zertifikat Enrollment Agent (EA) wird vom Administrator der Domänen-CA (Certificate Authority) ausgestellt.

Das Benutzerkonto, unter dem die PKI-Integration ausgeführt wird, muss den folgenden Kriterien entsprechen:

- Ist Domänenbenutzer.

- Ist lokaler Administrator des Geräts mit dem installierten Administrationsserver, von dem die PKI-Integration ausgeführt wird.

- Verfügt über die Berechtigung *Als Dienst anmelden*.

- Unter diesem Benutzerkonto muss zumindest einmal das Gerät mit dem installierten Administrationsserver gestartet werden, um ein ständiges Benutzerprofil zu erstellen.

Kaspersky Security Center Webserver

Der Kaspersky Security Center Webserver (Im Weiteren der Webserver) ist eine Komponente von Kaspersky Security Center. Der Webserver dient zur Veröffentlichung von autonomen Installationspaketen, autonomen Installationspaketen für mobile Geräte, iOS MDM-Profilen sowie Dateien aus dem freigegebenen Ordner.

Die erstellten iOS MDM-Profile und Installationspakete werden automatisch auf dem Webserver veröffentlicht und nach dem ersten Download gelöscht. Der Administrator kann den erstellten Link auf jede Weise an den Benutzer übermitteln, wie etwa per E-Mail.

Über diesem Link kann der Benutzer die für erforderlichen Informationen auf ein mobiles Gerät herunterladen.

Webserver-Einstellungen

Für die Feineinstellungen des Webservers ist in den Eigenschaften des Webservers der Verwaltungskonsole eine Möglichkeit zum Wechseln der Ports für die Protokolle HTTP (8060) und HTTPS (8061) vorgesehen. Ferner ist neben dem Wechsel der Ports der Wechsel des Serverzertifikats für das HTTPS-Protokoll und der Wechsel des FQDN-Namens des Webservers für das HTTP-Protokoll möglich.

Kaspersky Security Center installieren

In diesem Abschnitt wird die Installation der Komponenten von Kaspersky Security Center beschrieben. Wenn Sie die Programm nur auf einem lokalen Gerät installieren möchten, stehen Ihnen zwei Installationsmöglichkeiten zur Verfügung:

- **Standard**. Diese Option wird empfohlen, wenn Sie sich mit Kaspersky Security Center bekannt machen und die Ausführung des Programms z. B. in einem kleinen Bereich des Netzwerks testen möchten. Bei der Standardinstallation passen Sie nur die Einstellungen der Datenbank an. Bei der Standardinstallation konfigurieren Sie nur die Einstellungen der Datenbank und können nur den Standardsatz von Plug-ins zur Verwaltung der Kaspersky-Anwendungen installieren. Sie können die Standardinstallation auch verwenden, wenn Sie bereits Erfahrung mit Kaspersky Security Center haben und in der Lage sind, alle erforderlichen Einstellungen nach der Standardinstallation anzupassen.

- **Benutzerdefiniert**. Diese Option wird empfohlen, wenn Sie die Einstellungen von Kaspersky Security Center wie z. B. den Pfad zum freigegeben Ordner, Benutzerkonten und Ports für die Verbindung mit dem Administrationsserver sowie die Einstellungen der Datenbank ändern möchten. Bei der benutzerdefinierten Installation können Sie angeben, welche Verwaltungs-Plug-ins für Programme von Kaspersky installiert werden sollen. Falls erforderlich, können Sie die benutzerdefinierte Installation im Silent-Modus starten.

Wenn im Netzwerk zumindest ein Administrationsserver installiert ist, können die Server auf anderen Geräten des Netzwerkes mithilfe der Aufgabe zur Remote-Installation mit der Methode erzwungene Installation installiert werden. Beim Erstellen der Aufgabe zur Remote-Installation sollten Sie das Installationspaket des Administrationsservers verwenden: ksc_<Versionsnummer>.<Build-Nummer>_full_<Lokalisierungssprache>.exe.

Verwenden Sie dieses Paket, wenn Sie alle Komponenten, welche die vollständige Funktionalität von Kaspersky Security Center gewährleisten, installieren oder die bereits vorhandenen Versionen dieser Komponenten aktualisieren möchten.

Wenn Sie das Kaspersky Security Center Failover-Clusters bereitstellen möchten, müssen Sie Kaspersky Security Center auf allen Knoten des Clusters installieren.

Vorbereitung der Installation

Führen Sie die folgenden Maßnahmen aus, bevor Sie die Installation starten.

- **Überprüfen der Hardware- und Softwarevoraussetzungen**

  Vergewissern Sie sich, dass die Hard- und Softwarevoraussetzungen des Geräts den Anforderungen des Administrationsservers und der Verwaltungskonsole entsprechen.

- **Auswählen und installieren des Datenbankmanagementsystems (DBMS)**

  Kaspersky Security Center speichert seine Daten in einer Datenbank, die durch ein DBMS verwaltet wird. Installieren Sie das DBMS vor Kaspersky Security Center im Netzwerk (Weitere Informationen zum Auswählen eines DBMS). Wenn Sie sich entscheiden, PostgreSQL oder Postgres Pro als DBMS zu installieren, geben Sie ein Kennwort für den Superuser an. Wenn das Kennwort nicht angegeben wird, kann sich der Administrationsserver möglicherweise nicht mit der Datenbank verbinden.

  Es wird empfohlen, dass Sie den Administrationsserver anstatt auf einem Domänencontroller auf einem dezidierten Server installieren. Wenn Sie Kaspersky Security Center jedoch auf einem Server installieren, der als schreibgeschützter Domänencontroller (RODC) agiert, muss Microsoft SQL Server (SQL Express) nicht lokal (auf demselben Gerät) installiert werden. In diesem Fall empfehlen wir Ihnen, Microsoft SQL Server (SQL Express) per Fernzugriff (auf einem anderen Gerät) zu installieren, oder MySQL, MariaDB oder PostgreSQL zu verwenden, falls Sie das DBMS lokal installieren müssen.

- **Bereiten Sie Ordner für den Administrationsserver, den Administrationsagenten und die Verwaltungskonsole vor**

  Der Administrationsserver, Administrationsagent und die Verwaltungskonsole sollen in Ordner installiert werden, für welche die Unterscheidung von Groß- und Kleinschreibung deaktiviert ist. Die Unterscheidung von Groß- und Kleinschreibung muss außerdem für den freigegebenen Ordner des Administrationsservers und den versteckten Ordner von Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit) deaktiviert sein.

- **Entfernen Sie den alten Administrationsagenten**

  Mit der Komponente Administrationsserver wird die Serverversion des Administrationsagenten auf dem Gerät installiert. Eine Installation des Administrationsservers mit der üblichen Version des Administrationsagenten ist nicht möglich. Wenn bereits eine Serverversion des Administrationsagenten auf Ihrem Gerät installiert ist, deinstallieren Sie diese und starten Sie die Installation des Administrationsservers erneut. Einzelheiten zur Serverversion des Administrationsagenten finden Sie unter Änderungen im System nach der Installation von Kaspersky Security Center.

- **Überprüfen der Benutzerkonten**

  Zur Installation von Kaspersky Security Center werden die Rechte des lokalen Administrators auf dem Gerät verwendet, auf dem die Installation ausgeführt werden soll.

  Kaspersky Security Center unterstützt verwaltete Dienstkonten und gruppenverwaltete Dienstkonten. Wenn solche Benutzerkonten in Ihrer Domäne verwendet werden und Sie eines der Konten als Benutzerkonto für den Dienst des Administrationsservers angeben möchten, installieren Sie zunächst das Konto auf dem Gerät, auf dem Sie den Administrationsserver installieren möchten. Weitere Informationen zur Installation eines verwalteten Dienstkontos entnehmen Sie bitte der offiziellen Dokumentation von Microsoft.

Benutzerkonten für die Arbeit mit DBMS

Um den Administrationsserver zu installieren und damit zu arbeiten, benötigen Sie ein Windows-Konto, unter dem Sie das Installationsprogramm des Administrationsservers ausführen (im Folgenden auch als Installer bezeichnet), ein Windows-Konto, unter dem Sie den Dienst des Administrationsservers starten, und ein internes DBMS-Konto für den Zugriff auf das DBMS. Sie können neue Konten erstellen oder vorhandene verwenden. Alle Konten erfordern bestimmte Rechte. Ein Satz dieser benötigten Konten und deren Rechte hängt von folgenden Kriterien ab:

- DBMS-Typ:
  - Microsoft SQL Server (mit Windows-Authentifizierung oder SQL Server-Authentifizierung)
  - MySQL oder MariaDB
  - PostgreSQL oder Postgres Pro
- Speicherort des DBMS:
  - **Lokales DBMS**. Als *lokales DBMS* wird das DBMS bezeichnet, das auf demselben Gerät installiert ist wie der Administrationsserver.
  - **Remote-DBMS**. Als *Remote-DBMS* wird das DBMS bezeichnet, das auf einem anderen Gerät installiert ist.
- Methode zur Erstellung der Datenbank des Administrationsservers:
  - **Automatisch**. Während der Installation des Administrationsservers können Sie automatisch eine Datenbank für den Administrationsserver anlegen (auch als Serverdatenbank bezeichnet) indem Sie das Installationsprogramm verwenden.
  - **Manuell**. Sie können eine Anwendung eines Drittanbieters (z. B. SQL Server Management Studio) oder ein Skript verwenden, um eine leere Datenbank zu erstellen. Anschließend können Sie die Datenbank während der Installation des Administrationsservers als Serverdatenbank angeben.

Befolgen Sie das Prinzip der geringsten Rechte, wenn Sie den Konten Rechte und Berechtigungen erteilen. Das bedeutet, dass die gewährte Rechte gerade ausreichend sein sollten, um die erforderlichen Aktionen auszuführen.

Die folgenden Tabellen enthalten Informationen über die Systemrechte und DBMS-Rechte, die Sie den Konten gewähren sollten, bevor Sie den Administrationsserver installieren und starten.

Microsoft SQL Server mit Windows-Authentifizierung

Wenn Sie SQL Server als DBMS auswählen, können Sie die Windows-Authentifizierung verwenden, um auf SQL Server zuzugreifen. Konfigurieren Sie Systemrechte für ein Windows-Konto, das zum Ausführen des Installationsprogramms verwendet wird, und ein Windows-Konto, das zum Starten des Administrationsserver-Dienstes verwendet wird. Erstellen Sie auf SQL Server für diese beiden Windows-Konten jeweils einen Login. Gewähren Sie diesen Konten je nach Erstellungsmethode der Serverdatenbank die erforderlichen Rechte für SQL Server, wie in der folgenden Tabelle beschrieben. Weitere Informationen zum Konfigurieren der Kontoberechtigungen finden Sie unter Benutzerkonten für die Arbeit mit SQL Server konfigurieren (Windows-Authentifizierung).

DBMS: Microsoft SQL Server (einschließlich Express Edition) mit Windows-Authentifizierung

	Automatische Erstellung der Datenbank (mittels Installer)	Manuelle Erstellung der Datenbank (durch den Administrator)
Benutzerkonto, unter dem der Installer ausgeführt wird	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: ein lokales Administratorkonto oder ein Domänenkonto.	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: ein lokales Administratorkonto oder ein Domänenkonto.
Rechte des Benutzerkontos, in dessen Namen der Installer ausgeführt wird	• Systemrechte: Rechte des lokalen Administrators. • SQL Server-Rechte: • Rolle auf Server-Ebene: sysadmin.	• Systemrechte: Rechte des lokalen Administrators. • SQL Server-Rechte: • Rolle auf Server-Ebene: öffentlich. • Datenbankrolle für die Serverdatenbank: db_owner, public. • Standardschema für die Serverdatenbank: dbo.
Benutzerkonto für Dienst des Administrationsservers	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: • Ein vom Administrator ausgewähltes Windows-Benutzerkonto. • Ein Konto im Format "KL-AK-*", welches der Installer automatisch erstellt.	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: • Ein vom Administrator ausgewähltes Windows-Benutzerkonto. • Ein Konto im Format "KL-AK-*", welches der Installer automatisch erstellt (in diesem Fall wird es nicht empfohlen, dass Sie ein "KL-AK-*"-Konto erstellen).
Rechte des Benutzerkontos für den Dienst des Administrationsservers	• Systemrechte: Die erforderlichen Rechte werden vom Installer zugewiesen. • SQL Server-Rechte: Die erforderlichen Rechte werden vom Installer zugewiesen.	• Systemrechte: Die erforderlichen Rechte werden vom Installer zugewiesen. • SQL Server-Rechte: • Rolle auf Server-Ebene: öffentlich. • Datenbankrolle für die Serverdatenbank: db_owner, public. • Standardschema für die Serverdatenbank: dbo.

Microsoft SQL Server mit SQL Server-Authentifizierung

Wenn Sie SQL Server als DBMS auswählen, können Sie die SQL Server-Authentifizierung verwenden, um auf SQL Server zuzugreifen. Konfigurieren Sie Systemrechte für ein Windows-Konto, das zum Ausführen des Installationsprogramms verwendet wird, und ein Windows-Konto, das zum Starten des Administrationsserver-Dienstes verwendet wird. Erstellen Sie auf dem SQL Server eine Anmeldung mit einem Kennwort, um es für die Authentifizierung zu verwenden. Gewähren Sie anschließend diesem SQL Server-Konto die erforderlichen Rechte, die in der folgenden Tabelle aufgeführt sind. Weitere Informationen zum Konfigurieren der Kontoberechtigungen finden Sie unter Benutzerkonten für die Arbeit mit SQL Server konfigurieren (SQL Server-Authentifizierung).

DBMS: Microsoft SQL Server (einschließlich Express Edition) mit SQL Server-Authentifizierung

	Automatische Erstellung der Datenbank (mittels Installer)	Manuelle Erstellung der Datenbank (durch den Administrator)
Benutzerkonto, unter dem der Installer ausgeführt wird	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: ein lokales Administratorkonto oder ein Domänenkonto.	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: ein lokales Administratorkonto oder ein Domänenkonto.

	Automatische Erstellung der Datenbank (mittels Installer)	Manuelle Erstellung der Datenbank (durch den Administrator)
Rechte des Benutzerkontos, in dessen Namen der Installer ausgeführt wird	Systemrechte: Rechte des lokalen Administrators.	Systemrechte: Rechte des lokalen Administrators.
Benutzerkonto für Dienst des Administrationsservers	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: • Ein vom Administrator ausgewähltes Windows-Benutzerkonto. • Ein Konto im Format "KL-AK-*", welches der Installer automatisch erstellt.	• Remote-DBMS: nur ein Domänenkonto für das Remote-Gerät, auf dem das DBMS installiert ist. • Lokales DBMS: • Ein vom Administrator ausgewähltes Windows-Benutzerkonto. • Ein Konto im Format "KL-AK-*", welches der Installer automatisch erstellt.
Rechte des Benutzerkontos für den Dienst des Administrationsservers	Systemrechte: Die erforderlichen Rechte werden vom Installer zugewiesen.	Systemrechte: Die erforderlichen Rechte werden vom Installer zugewiesen.
Rechte des Anmeldenamens, der für die SQL Server-Authentifizierung verwendet wird	Erforderliche SQL Server-Rechte zum Erstellen einer Datenbank und Installieren des Administrationsservers: • Rolle auf Server-Ebene: öffentlich. • Datenbankrolle für die Datenbank *Master*: db_owner. • Standardschema für die *Master*-Datenbank: dbo. • Berechtigungen: • CONNECT ANY DATABASE • CONNECT SQL • CREATE ANY DATABASE • VIEW ANY DATABASE • VIEW SERVER STATE (bei aktivierter Option **Always On**) Erforderliche SQL Server-Rechte für die Arbeit mit dem Administrationsserver: • Rolle auf Server-Ebene: öffentlich. • Datenbankrolle für die Serverdatenbank: db_owner. • Standardschema für die Serverdatenbank: dbo. • Berechtigungen: • CONNECT SQL • VIEW ANY DATABASE • VIEW SERVER STATE (bei aktivierter Option **Always On**) • VIEW ANY DEFINITION	SQL Server-Rechte: • Rolle auf Server-Ebene: öffentlich. • Datenbankrolle für die Serverdatenbank: db_owner. • Standardschema für die Serverdatenbank: dbo. • Berechtigungen: • CONNECT SQL • VIEW ANY DATABASE • VIEW ANY DEFINITION

Konfigurieren der SQL Server-Rechte für die Wiederherstellung der Daten des Administrationsservers

Um die Daten des Administrationsservers aus der Sicherung wiederherzustellen, starten Sie das Tool "klbackup" unter dem Windows-Konto, das zur Installation des Administrationsservers verwendet wurde. Gewähren Sie vor dem Ausführen des Tools "klbackup" auf dem SQL Server die Rechte für den SQL Server-Login, der diesem Windows-Konto zugeordnet ist. Die SQL Server-Rechte unterscheiden sich je nach Version des Administrationsservers. Für den Administrationsserver ab Version 14.2 können Sie die Rolle sysadmin auf Serverebene oder die Rolle dbcreator auf Serverebene zuweisen.

Berechtigungen von SQL Server für die Wiederherstellung der Administrationsserver-Datenbank

Administrationsserver ab Version 14.2	Andere Versionen des Administrationsservers
• SQL Server-Rechte: • Rolle auf Server-Ebene: dbcreator. • Berechtigungen: • VIEW ANY DEFINITION Geben Sie vor dem Ausführen des Tools "klbackup" das Server-Flag KLSRV_SKIP_ADJUSTING_DBMS_ACCESS an. Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center". Führen Sie anschließend den folgenden Befehl in der Befehlszeile aus: `klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL und MariaDB

Wenn Sie MySQL oder MariaDB als DBMS auswählen, erstellen Sie ein internes DBMS-Konto und gewähren Sie diesem Konto die erforderlichen Rechte, die in der folgenden Tabelle aufgeführt sind. Das Installationsprogramm und der Dienst des Administrationsservers verwenden dieses interne DBMS-Konto für den Zugriff auf das DBMS. Beachten Sie, dass die Art der Datenbankerstellung keinen Einfluss auf den erforderlichen Satz an Berechtigungen hat. Weitere Informationen zum Konfigurieren der Kontoberechtigungen finden Sie unter Benutzerkonten für die Arbeit mit MySQL und MariaDB konfigurieren.

DBMS: MySQL und MariaDB

	Automatische oder manuelle Datenbankerstellung
Benutzerkonto, unter dem der Installer ausgeführt wird	• Remote-DBMS: Nur ein Domänenkonto für das Remote-Gerät mit installiertem DBMS. • Lokales DBMS: ein lokales Administratorkonto oder ein Domänenkonto.
Rechte des Benutzerkontos, in dessen Namen der Installer ausgeführt wird	Systemrechte: Rechte des lokalen Administrators.
Benutzerkonto für Dienst des Administrationsservers	• Remote-DBMS: Nur ein Domänenkonto für das Remote-Gerät mit installiertem DBMS. • Lokales DBMS: • Ein vom Administrator ausgewähltes Windows-Benutzerkonto. • Ein Konto im Format "KL-AK-*", das der Installer automatisch erstellt.
Rechte des Benutzerkontos für den Dienst des Administrationsservers	Systemrechte: Die erforderlichen Rechte werden vom Installer zugewiesen.
Rechte des internen DBMS-Kontos	Schema-Privilegien: • Administrationsserver-Datenbank: ALL (außer GRANT OPTION). • Systemschemata (mysql und sys): SELECT, SHOW VIEW. • Gespeicherte Prozedur sys.table_exists: EXECUTE (wenn Sie MariaDB 10.5 oder früher als DBMS verwenden, müssen Sie das EXECUTE-Privileg nicht erteilen). Globale Privilegien für alle Schemata: PROCESS, SUPER.

Ausführliche Informationen zum Verschieben von Daten aus einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich finden Sie unter Verschieben von Daten aus einem freigegebenen Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich in MySQL und MariaDB-DBMS.

Berechtigungen für die Wiederherstellung der Daten des Administrationsservers konfigurieren

Die Rechte, die Sie dem internen DBMS-Konto erteilt haben, reichen aus, um die Daten des Administrationsservers aus der Sicherung wiederherzustellen. Um die Wiederherstellung zu starten, führen Sie das Dienstprogramm klbackup unter dem Windows-Konto aus, das zur Installation des Administrationsservers verwendet wurde.

PostgreSQL oder Postgres Pro

Wenn Sie PostgreSQL oder Postgres Pro als DBMS auswählen, können Sie den Benutzer *Postgres* (die standardmäßige Postgres-Rolle) verwenden oder eine neue Postgres-Rolle (im Folgenden auch als Rolle bezeichnet) erstellen, um auf das DBMS zuzugreifen. Gewähren Sie der Rolle je nach Erstellungsmethode der Serverdatenbank die erforderlichen Rechte, wie in der folgenden Tabelle beschrieben. Weitere Informationen zum Konfigurieren der Rollenberechtigung finden Sie unter Benutzerkonten für die Arbeit mit PostgreSQL oder Postgres Pro konfigurieren.

DBMS: PostgreSQL oder Postgres Pro

	Automatische Datenbankerstellung		Manuelle Datenbankerstellung
Benutzerkonto, unter dem der Installer ausgeführt wird	• Remote-DBMS: Nur ein Domänenkonto für das Remote-Gerät mit installiertem DBMS. • Lokales DBMS: ein lokales Administratorkonto oder ein Domänenkonto.		• Remote-DBMS: Nur ein Domänenkonto für das Remote-Gerät mit installiertem DBMS. • Lokales DBMS: ein lokales Administratorkonto oder ein Domänenkonto.
Rechte des Benutzerkontos, in dessen Namen der Installer ausgeführt wird	Systemrechte: Rechte des lokalen Administrators.		Systemrechte: Rechte des lokalen Administrators.
Benutzerkonto für Dienst des Administrationsservers	• Remote-DBMS: Nur ein Domänenkonto für das Remote-Gerät mit installiertem DBMS. • Lokales DBMS: • Ein vom Administrator ausgewähltes Windows-Benutzerkonto. • Ein Konto im Format "KL-AK-*", das der Installer automatisch erstellt.		• Remote-DBMS: Nur ein Domänenkonto für das Remote-Gerät mit installiertem DBMS. • Lokales DBMS: • Ein vom Administrator ausgewähltes Windows-Benutzerkonto. • Ein Konto im Format "KL-AK-*", das der Installer automatisch erstellt.
Rechte des Benutzerkontos für den Dienst des Administrationsservers	Systemrechte: Die erforderlichen Rechte werden vom Installer zugewiesen.		Systemrechte: Die erforderlichen Rechte werden vom Installer zugewiesen.
Rechte der Postgres-Rolle	Der Benutzer *Postgres* benötigt keine weiteren Rechte.	Privilegien für eine neue Rolle: `CREATEDB`.	Für eine neue Rolle: • Privilegien für die Administrationsserver-Datenbank: `ALL`. • Privilegien für alle Tabellen im Schema "public" `ALL`. • Privilegien für alle Sequenzen im Schema "public": `ALL`.

Berechtigungen für die Wiederherstellung der Daten des Administrationsservers konfigurieren

Um die Daten des Administrationsservers aus der Sicherung wiederherzustellen, starten Sie das Tool "klbackup" unter dem Windows-Konto, das zur Installation des Administrationsservers verwendet wurde. Beachten Sie, dass die Postgres-Rolle, die für den Zugriff auf das DBMS verwendet wird, über die Berechtigung "Owner" für die Administrationsserver-Datenbank verfügen muss.

Benutzerkonten für die Arbeit mit SQL Server konfigurieren (Windows-Authentifizierung)

Erforderliche Vorrausetzungen

Bevor Sie den Benutzerkonten Rechte zuweisen, führen Sie die folgenden Maßnahmen aus:

1. Stellen Sie sicher, dass Sie unter dem lokalen Administratorkonto am System angemeldet sind.
2. Installieren Sie eine geeignete Umgebung für die Arbeit mit SQL Server.

3. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Administrationsserver installieren.

4. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Dienst des Administrationsservers starten.

5. Erstellen Sie auf dem SQL-Server einen Login für das Windows-Konto, das zum Ausführen des Installationsprogramms des Administrationsservers (im Folgenden auch als Installer bezeichnet) verwendet wird. Erstellen Sie außerdem einen Login für das Windows-Konto, das für den Start des mit dem Administrationsserver-Dienstes verwendet wird.

Wenn Sie SQL Server Management Studio verwenden, wählen Sie auf der Seite **Allgemein** des Fensters mit den Anmeldeeigenschaften die Option **Windows-Authentifizierung**.

Wenn Sie den Administrationsserver und den SQL Server auf Geräten installieren möchten, die sich in separaten Windows-Domänen befinden, beachten Sie, dass diese Domänen über eine bidirektionale Vertrauensstellung verfügen müssen. Dies wird benötigt, um den ordnungsgemäßen Betrieb des Administrationsservers, einschließlich der Ausführung von Aufgaben und der Anwendung von Richtlinien, zu gewährleisten. Informationen über die erforderlichen Benutzerkonten für die Arbeit mit verschiedenen DBMS und über die Benutzerberechtigungen finden Sie unter Benutzerkonten für die Arbeit mit dem DBMS.

Konfigurieren der Konten für die Installation des Administrationsservers (automatisches Erstellen der Administrationsserver-Datenbank)

So konfigurieren Sie die Konten für die Installation des Administrationsservers:

1. Weisen Sie auf SQL Server dem Login des Windows-Kontos, das zum Ausführen des Installers verwendet wird, die Rolle "sysadmin" auf Serverebene zu.

2. Melden Sie sich beim System unter dem Windows-Konto an, das zum Ausführen des Installationsprogramms verwendet wurde.

3. Führen Sie das Installationsprogramm des Administrationsservers aus.

   Der Installationsassistent zum Einrichten des Administrationsservers wird gestartet. Folgen Sie den Anweisungen des Assistenten.

4. Wählen Sie die Option Benutzerdefinierte Installation des Administrationsservers aus.

5. Wählen Sie den Microsoft SQL Server als DBMS aus, der die Administrationsserver-Datenbank speichert.

6. Wählen Sie den Microsoft Windows-Authentifizierungsmodus aus, um über ein Windows-Konto eine Verbindung zwischen dem Administrationsserver und dem SQL Server herzustellen.

7. Geben Sie das Windows-Konto an, das zum Starten des Dienstes des Administrationsservers verwendet wird.

   Sie können das Windows-Benutzerkonto auswählen, für das Sie zuvor eine SQL Server-Anmeldung erstellt haben. Alternativ können Sie mit dem Installer automatisch ein neues Windows-Konto im "KL-AK-*"-Format erstellen. In diesem Fall erstellt das Installationsprogramm automatisch eine SQL Server-Anmeldung für dieses Konto. Unabhängig von der Wahl des Kontos weist der Installer dem Dienstkonto des Administrationsservers die erforderlichen Rechte für das System und SQL Server zu.

Nach Abschluss der Installation wird die Serverdatenbank erstellt und alle erforderlichen Rechte für das System und SQL Server werden dem Konto des Administrationsservers zugewiesen. Der Administrationsserver ist einsatzbereit.

Konfigurieren der Konten für die Installation des Administrationsservers (manuelles Erstellen der Administrationsserver-Datenbank)

So konfigurieren Sie die Konten für die Installation des Administrationsservers:

1. Erstellen Sie auf SQL Server eine leere Datenbank. Diese Datenbank wird als Administrationsserver-Datenbank verwendet (im Folgenden auch als Serverdatenbank bezeichnet).
2. Geben Sie für die beiden SQL Server-Logins, die für die Windows-Konten erstellt wurden, die Rolle "public" auf Serverebene an und konfigurieren Sie anschließend die Zuordnung zur erstellten Datenbank:
   - Rolle auf Server-Ebene: public
   - Datenbankrollen: db_owner, public
   - Standardschema: dbo
3. Melden Sie sich beim System unter dem Windows-Konto an, das zum Ausführen des Installationsprogramms verwendet wurde.
4. Führen Sie das Installationsprogramm des Administrationsservers aus.

   Der Installationsassistent zum Einrichten des Administrationsservers wird gestartet. Folgen Sie den Anweisungen des Assistenten.
5. Wählen Sie die Option Benutzerdefinierte Installation des Administrationsservers aus.
6. Wählen Sie den Microsoft SQL Server als DBMS aus, der die Datenbank des Administrationsservers speichert.
7. Geben Sie für den Namen der Administrationsserver-Datenbank den Namen der erstellten Datenbank an.
8. Wählen Sie den Microsoft Windows-Authentifizierungsmodus aus, um über ein Windows-Konto eine Verbindung zwischen dem Administrationsserver und dem SQL Server herzustellen.
9. Geben Sie das Windows-Konto an, das zum Starten des Dienstes des Administrationsservers verwendet wird.

   Sie können das Windows-Benutzerkonto auswählen, für das Sie zuvor eine SQL Server-Anmeldung erstellt und die Anmelderechte konfiguriert haben.

Es wird davon abgeraten, automatisch ein neues Windows-Konto im "KL-AK-*"-Format zu erstellen. In diesem Fall erstellt das Installationsprogramm ein neues Windows-Konto, für das Sie kein SQL Server-Konto erstellt und konfiguriert haben. Der Administrationsserver kann dieses Konto nicht zum Starten des Dienstes des Administrationsservers verwenden. Wenn es notwendig ist, ein "KL-AK-*"–Windows-Konto zu erstellen, starten Sie die Verwaltungskonsole nach der Installation nicht. Gehen Sie stattdessen wie folgt vor:

1. Stoppen Sie den Dienst "kladminserver".
2. Erstellen Sie einen SQL Server-Login für das erstellte "KL-AK-*"–Windows-Konto.

3. Gewähren Sie diesem SQL Server-Login die Rechte und konfigurieren Sie die Zuordnung zur erstellten Datenbank:
   - Rolle auf Server-Ebene: public
   - Datenbankrollen: db_owner, public
   - Standardschema: dbo
4. Starten Sie den Dienst "kladminserver" neu und starten Sie anschließend die Verwaltungskonsole.

Nach Abschluss der Installation verwendet der Administrationsserver die erstellte Datenbank zum Speichern der Serverdaten. Der Administrationsserver ist einsatzbereit.

Benutzerkonten für die Arbeit mit SQL Server konfigurieren (SQL Server-Authentifizierung)

Erforderliche Vorrausetzungen

Bevor Sie den Benutzerkonten Rechte zuweisen, führen Sie die folgenden Maßnahmen aus:

1. Stellen Sie sicher, dass Sie unter dem lokalen Administratorkonto am System angemeldet sind.
2. Installieren Sie eine geeignete Umgebung für die Arbeit mit SQL Server.
3. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Administrationsserver installieren.
4. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Dienst des Administrationsservers starten.
5. Aktivieren Sie auf SQL Server den SQL Server-Authentifizierungsmodus.

   Wenn Sie SQL Server Management Studio verwenden, wählen Sie im Eigenschaftenfenster von SQL Server auf der Seite **Sicherheit** die Option **SQL Server- und Windows-Authentifizierungsmodus**.
6. Erstellen Sie auf SQL Server einen Login mit einem Kennwort. Das Installationsprogramm des Administrationsservers (im Folgenden auch als Installer bezeichnet) und der Dienst des Administrationsservers verwenden diesen interne SQL Server-Login für den Zugriff auf SQL Server.

   Wenn Sie SQL Server Management Studio verwenden, wählen Sie auf der Seite **Allgemein** des Fensters mit den Anmeldeeigenschaften die Option **SQL Server-Authentifizierung**.

Wenn Sie den Administrationsserver und den SQL Server auf Geräten installieren möchten, die sich in separaten Windows-Domänen befinden, beachten Sie, dass diese Domänen über eine bidirektionale Vertrauensstellung verfügen müssen. Dies wird benötigt, um den ordnungsgemäßen Betrieb des Administrationsservers, einschließlich der Ausführung von Aufgaben und der Anwendung von Richtlinien, zu gewährleisten. Informationen über die erforderlichen Benutzerkonten für die Arbeit mit verschiedenen DBMS und über die Benutzerberechtigungen finden Sie unter Benutzerkonten für die Arbeit mit dem DBMS.

Konfigurieren der Konten für die Installation des Administrationsservers (automatisches Erstellen der Administrationsserver-Datenbank)

So konfigurieren Sie die Konten für die Installation des Administrationsservers:

1. Ordnen Sie auf SQL Server das SQL Server-Konto dem Standardkonto der *Master*-Datenbank zu. Die Datenbank *master* stellt ein Template für die Administrationsserver-Datenbank dar (im Folgenden auch als Serverdatenbank bezeichnet). Die Datenbank *master* wird solange für die Zuordnung verwendet, bis der Installer eine Serverdatenbank erstellt hat. Gewähren Sie dem SQL Server-Konto die folgenden Rechte und Berechtigungen:

   - Rolle auf Server-Ebene: public
   - Datenbankrolle für die Datenbank *master*: db_owner
   - Standardschema für die Datenbank *master*: dbo
   - Berechtigungen:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE

2. Melden Sie sich beim System unter dem Windows-Konto an, das zum Ausführen des Installationsprogramms verwendet wurde.

3. Starten Sie den Installer.

   Der Installationsassistent zum Einrichten des Administrationsservers wird gestartet. Folgen Sie den Anweisungen des Assistenten.

4. Wählen Sie die Option Benutzerdefinierte Installation des Administrationsservers aus.

5. Wählen Sie den Microsoft SQL Server als DBMS aus, der die Datenbank des Administrationsservers speichert.

6. Geben Sie den Namen der Administrationsserver-Datenbank an.

7. Wähle Sie den SQL Server-Authentifizierungsmodus aus, um eine Verbindung zwischen dem Administrationsserver und SQL Server über das erstellte SQL Server-Konto herzustellen. Geben Sie anschließend die Anmeldeinformationen für das SQL Server-Konto an.

8. Geben Sie das Windows-Konto an, das zum Starten des Dienstes des Administrationsservers verwendet wird.

   Sie können ein vorhandenes Windows-Benutzerkonto auswählen oder mithilfe des Installers ein neues Windows-Konto im "KL-AK-*"-Format erstellen. Unabhängig von der Kontoauswahl weist der Installer dem Dienstkonto des Administrationsservers die erforderlichen Systemrechte zu.

Nach Abschluss der Installation wird die Serverdatenbank erstellt und alle erforderlichen Rechte für das System werden dem Konto des Administrationsservers zugewiesen. Der Administrationsserver ist einsatzbereit.

Sie können die Zuordnung zur *Master*-Datenbank aufheben, da das Installationsprogramm während der Installation des Administrationsservers eine Serverdatenbank erstellt und die Zuordnung zu dieser Datenbank konfiguriert hat.

Da die automatische Datenbankerstellung mehr Berechtigungen erfordert als die gewöhnliche Arbeit mit dem Administrationsserver, können Sie einige Berechtigungen aufheben. Wählen Sie auf dem SQL Server das SQL Server-Konto aus und gewähren Sie anschließend die folgenden Rechte für die Arbeit mit dem Administrationsserver:

- Rolle auf Server-Ebene: public
- Datenbankrolle für die Serverdatenbank: db_owner
- Standardschema für die Serverdatenbank: dbo
- Berechtigungen:
  - CONNECT SQL
  - VIEW ANY DATABASE

Konfigurieren der Konten für die Installation des Administrationsservers (manuelles Erstellen der Datenbank des Administrationsservers)

So konfigurieren Sie die Konten für die Installation des Administrationsservers:

1. Erstellen Sie auf SQL Server eine leere Datenbank. Diese Datenbank wird als Administrationsserver-Datenbank verwendet.
2. Gewähren Sie auf SQL Server dem SQL Server-Konto die folgenden Rechte und Berechtigungen:
   - Rolle auf Server-Ebene: öffentlich.
   - Datenbankrollen für die erstellte Datenbank: db_owner.
   - Standardschema für die erstellte Datenbank: dbo.
   - Berechtigungen:
     - CONNECT SQL
     - VIEW ANY DATABASE
3. Melden Sie sich beim System unter dem Windows-Konto an, das zum Ausführen des Installationsprogramms verwendet wurde.
4. Starten Sie den Installer.

   Der Installationsassistent zum Einrichten des Administrationsservers wird gestartet. Folgen Sie den Anweisungen des Assistenten.
5. Wählen Sie die Option Benutzerdefinierte Installation des Administrationsservers aus.
6. Wählen Sie den Microsoft SQL Server als DBMS aus, der die Datenbank des Administrationsservers speichert.
7. Geben Sie für den Namen der Administrationsserver-Datenbank den Namen der erstellten Datenbank an.

8. Wähle Sie den SQL Server-Authentifizierungsmodus aus, um eine Verbindung zwischen dem Administrationsserver und SQL Server über das erstellte SQL Server-Konto herzustellen. Geben Sie anschließend die Anmeldeinformationen für das SQL Server-Konto an.

9. Geben Sie das Windows-Konto an, das zum Starten des Dienstes des Administrationsservers verwendet wird.

   Sie können ein vorhandenes Windows-Benutzerkonto auswählen oder mithilfe des Installers ein neues Windows-Konto im "KL-AK-*"-Format erstellen. Unabhängig von der Kontoauswahl weist der Installer dem Dienstkonto des Administrationsservers die erforderlichen Systemrechte zu.

Nach Abschluss der Installation verwendet der Administrationsserver die erstellte Datenbank zum Speichern der Daten des Administrationsservers. Alle erforderlichen Rechte für das System werden dem Dienstkonto des Administrationsservers zugewiesen. Der Administrationsserver ist einsatzbereit.

Benutzerkonten für die Arbeit mit MySQL und MariaDB konfigurieren

Erforderliche Vorrausetzungen

Bevor Sie den Benutzerkonten Rechte zuweisen, führen Sie die folgenden Maßnahmen aus:

1. Stellen Sie sicher, dass Sie unter dem lokalen Administratorkonto am System angemeldet sind.

2. Installieren Sie eine geeignete Umgebung für die Arbeit mit MySQL oder MariaDB.

3. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Administrationsserver installieren.

4. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Dienst des Administrationsservers starten.

Konfigurieren der Benutzerkonten, um den Administrationsserver zu installieren

So konfigurieren Sie die Konten für die Installation des Administrationsservers:

1. Führen Sie eine Umgebung zum Arbeiten mit MySQL oder MariaDB unter dem Root-Konto aus, das Sie bei der Installation des DBMS erstellt haben.

2. Erstellen Sie ein internes DBMS-Konto mit einem Passwort. Das Installationsprogramm des Administrationsservers (im Folgenden auch als Installer bezeichnet) und der Dienst des Administrationsservers des Administrationsservers verwenden dieses interne DBMS-Konto für den Zugriff auf das DBMS. Gewähren Sie diesem Konto die folgenden Berechtigungen:

   - Schema-Privilegien:
     - Administrationsserver-Datenbank: ALL (außer `GRANT OPTION`)
     - Systemschemata (mysql und sys): `SELECT`, `SHOW VIEW`
     - Die gespeicherte Prozedur sys.table_exists: `EXECUTE`
   - Globale Privilegien für alle Schemata: `PROCESS`, `SUPER`

Um ein internes DBMS-Konto zu erstellen und diesem Konto die erforderlichen Berechtigungen zu erteilen, führen Sie das folgende Skript aus (in diesem Skript lautet der DBMS-Login *KSCAdmin* und der Name der Administrationsserver-Datenbank *kav*):

```
/* Anlegen eines Benutzers namens KSCAdmin */
CREATE USER 'KSCAdmin'
/* Angeben des Kennworts für KSCAdmin */
IDENTIFIED BY '<Kennwort>';
```

Wenn Sie MySQL 8.0 oder früher als DBMS verwenden, beachten Sie, dass für diese Versionen die "Caching SHA2 password"-Authentifizierung nicht unterstützt wird. Ändern Sie die Standardauthentifizierung von "Caching SHA2 password" in "MySQL native password":

- Führen Sie den folgenden Befehl aus, um ein DBMS-Konto zu erstellen, das die "MySQL native password"-Authentifizierung verwendet:

  ```
  CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<Kennwort>';
  ```

- Führen Sie den folgenden Befehl aus, um die Authentifizierung für ein vorhandenes DBMS-Konto zu ändern:

  ```
  ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<Kennwort>';
  ```

```
/* KSCAdmin Berechtigungen gewähren */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

> Wenn Sie MariaDB 10.5 oder früher als DBMS verwenden, müssen Sie das EXECUTE-Privileg nicht erteilen. Schließen Sie in diesem Fall den folgenden Befehl aus dem Skript aus: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Führen Sie das folgende Skript aus, um die Liste der Berechtigungen anzuzeigen, die dem DBMS-Konto gewährt wurden:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Um eine Administrationsserver-Datenbank manuell zu erstellen, führen Sie das folgende Skript aus (in diesem Skript lautet der Name der Administrationsserver-Datenbank *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Verwenden Sie denselben Datenbanknamen, den Sie in dem Skript angeben, welches das DBMS-Konto erstellt.

5. Melden Sie sich beim System unter dem Windows-Konto an, das zum Ausführen des Installationsprogramms verwendet wurde.

6. Starten Sie den Installer.

   Der Installationsassistent zum Einrichten des Administrationsservers wird gestartet. Folgen Sie den Anweisungen des Assistenten.

7. Wählen Sie die Option Benutzerdefinierte Installation des Administrationsservers aus.

8. Wählen Sie MySQL oder MariaDB als DBMS aus, in dem die Administrationsserver-Datenbank gespeichert ist.

9. Geben Sie den Datenbanknamen des Administrationsservers an. Verwenden Sie denselben Datenbanknamen, den Sie im Skript angeben.

10. Geben Sie die Anmeldeinformationen des DBMS-Kontos an, dass Sie durch das Skript erstellt haben.

11. Geben Sie das Windows-Konto an, das zum Starten des Dienstes des Administrationsservers verwendet wird.

    Sie können ein vorhandenes Windows-Benutzerkonto auswählen oder mithilfe des Installers automatisch ein neues Windows-Konto im "KL-AK-*"-Format erstellen. Unabhängig von der Kontoauswahl weist der Installer dem Dienstkonto des Administrationsservers die erforderlichen Systemrechte zu.

Nach Abschluss der Installation wird die Datenbank des Administrationsservers erstellt und der Administrationsserver ist einsatzbereit.

In MySQL und MariaDB-DBMS Daten aus einem freigegebenen Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschieben

Für ein MySQL- und MariaDB-DBMS können Sie Daten auf folgende Weise speichern:

- Als gemeinsam genutzter Tabellenbereich, wenn die Daten aller Benutzer-Datenbanken in einer einzigen Datei gespeichert sind (normalerweise in der Datei `ibdata1`).
- Als Tabellenbereich für Dateien pro Tabelle, wenn für jede Tabelle ein separater Datenbereich als separate Datei erstellt wird.

Die Verwendung eines gemeinsam genutzten Tabellenbereichs erhöht das Risiko der Fragmentierung des Tabellenbereichs. Da es nicht möglich ist, eine `SHRINK` -Operation auszuführen, kann eine Datei in einem gemeinsam genutzten Tabellenbereich etwa 90 % des Speicherplatzes einnehmen. Dies wirkt sich negativ auf die Leistung des Datenträgersubsystems aus. Daher ist es sinnvoll, sich für einen Tabellenbereich für Dateien pro Tabelle zu entscheiden.

In diesem Artikel wird beschrieben, wie Sie Daten aus einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschieben. Wenn das MySQL- oder MariaDB-DBMS auch von anderen Anwendungen verwendet wird, müssen Sie die Datenbanken dieser Anwendungen in den Datei-pro-Tabelle-Tabellenbereich verschieben.

> Es wird empfohlen, dieses Verfahren nur auszuführen, wenn Sie ein MySQL- oder MariaDB-DBMS für den Administrationsserver verwenden.
> Das Verschieben von Daten aus einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich kann die Belastung des Festplatten-Subsystems erhöhen.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie Folgendes sicher:

- Sie haben eine Backup-Kopie der Daten des Administrationsservers erstellt, indem Sie entweder eine Aufgabe zur Datensicherung oder das Tool klbackup ausgeführt haben.
- Sie haben eine Backup-Kopie anderer Anwendungen erstellt, deren Anwendungsdatenbanken von einem MySQL- oder MariaDB-DBMS (falls vorhanden) verwaltet werden.
- Auf dem Gerät, auf dem das DBMS installiert ist, ist in der Partition mit der Datenbank freier Speicherplatz auf der Festplatte vorhanden.

Der erforderliche Speicherplatz beträgt 150 % der aktuellen Gesamtgröße der Datenbanken (aktuelle Größe der Datei `ibdata1`).

Prozess

Gehen Sie wie folgt vor, um Daten aus einem gemeinsam genutzten Tabellenbereich in einen Tabellenbereich für Dateien pro Tabelle zu verschieben:

1. Stoppen Sie den Kaspersky Security Center Administrationsserver und andere Anwendungen, welche die gleiche DBMS-Instanz verwenden, für die Sie diesen Vorgang ausführen möchten.
2. Melden Sie sich je nach DBMS-Version als Superuser an Ihrem DBMS an und führen Sie anschließend in einer beliebigen Anwendung das Skript `fix_tablespace.sql` aus.

   Sie können die Skripte `fix_tablespace.sql` anzeigen, indem Sie auf diese Links klicken:

   Das Skript für MySQL 5.7 und MariaDB 10.1+ anzeigen

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

   Das Skript für MySQL 8.0+ anzeigen

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
```

```
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Sie dürfen die Skriptausführung nicht stoppen.
Wenn keine DBMS-Fehler aufgetreten sind, Sie aber die Skriptausführung beendet haben, führen Sie entweder das Skript erneut durch oder stoppen Sie die Schritte dieses Verfahrens, starten Sie den DBMS-Dienst neu und stellen Sie die Daten des Administrationsservers aus der Sicherung wieder her.

3. Setzen Sie im Abschnitt `[mysqld]` der Datei my.cnf den Parameter `innodb_file_per_table` auf `1`.
4. Starten Sie den MySQL oder MariaDB-Dienst neu.
5. Starten Sie den Dienst des Kaspersky Security Center Administrationsservers neu.

Die Daten werden von einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschoben.

Benutzerkonten für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren

Erforderliche Vorrausetzungen

Bevor Sie den Benutzerkonten Rechte zuweisen, führen Sie die folgenden Maßnahmen aus:

1. Stellen Sie sicher, dass Sie unter dem lokalen Administratorkonto am System angemeldet sind.
2. Installieren Sie eine geeignete Umgebung für die Arbeit mit PostgreSQL und Postgres Pro.
3. PostgresSQL- oder Postgres Pro-Server für die Arbeit mit Kaspersky Security Center 15.1 konfigurieren.

4. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Administrationsserver installieren.

5. Stellen Sie sicher, dass Sie über ein Windows-Konto verfügen, unter dem Sie den Dienst des Administrationsservers starten.

Konfigurieren der Konten für die Installation des Administrationsservers (automatisches Erstellen der Datenbank des Administrationsservers)

So konfigurieren Sie die Konten für die Installation des Administrationsservers:

1. Starten Sie eine Umgebung für die Arbeit mit PostgreSQL und Postgres Pro.

2. Wählen Sie eine Postgres-Rolle aus, um auf das DBMS zuzugreifen. Sie können eine der folgenden Rollen verwenden:

   - Den Benutzer *Postgres* (standardmäßige Postgres-Rolle).

     Wenn Sie den Benutzer *Postgres* verwenden, müssen Sie ihm keine zusätzlichen Rechte gewähren.

   - Eine neue Postgres-Rolle.

     Wenn Sie eine neue Postgres-Rolle verwenden möchten, erstellen Sie diese Rolle und erteilen Sie ihr anschließend das Privileg CREATEDB. Führen Sie dazu folgendes Skript aus (in diesem Skript lautet die Rolle *KSCAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<password>' CREATEDB;
     ```

     Die erstellte Rolle wird als Besitzer der Datenbank des Administrationsservers (im Folgenden auch als Serverdatenbank bezeichnet) verwendet.

3. Melden Sie sich am System unter dem Windows-Benutzerkonto an, mit dem das Installationsprogramm des Administrationsservers ausgeführt wird (im Folgenden auch als Installer bezeichnet).

4. Starten Sie den Installer.

   Der Installationsassistent zum Einrichten des Administrationsservers wird gestartet. Folgen Sie den Anweisungen des Assistenten.

5. Wählen Sie die Option Benutzerdefinierte Installation des Administrationsservers aus.

6. Wählen Sie PostgreSQL oder Postgres Pro als DBMS aus, in dem die Administrationsserver-Datenbank gespeichert wird.

7. Geben Sie den Namen der Serverdatenbank an. Der Installer erstellt die Serverdatenbank automatisch.

8. Geben Sie die Anmeldeinformationen der Postgres-Rolle an.

9. Geben Sie das Windows-Konto an, das zum Starten des Dienstes des Administrationsservers verwendet wird.

   Sie können ein vorhandenes Windows-Benutzerkonto auswählen oder mithilfe des Installers automatisch ein neues Windows-Konto im "KL-AK-*"-Format erstellen. Unabhängig von der Kontoauswahl weist der Installer dem Dienstkonto des Administrationsservers die erforderlichen Systemrechte zu.

Nach Abschluss der Installation wird die Serverdatenbank automatisch erstellt und der Administrationsserver ist einsatzbereit.

Konfigurieren der Konten für die Installation des Administrationsservers (manuelles Erstellen der Datenbank des Administrationsservers)

So konfigurieren Sie die Konten für die Installation des Administrationsservers:

1. Starten Sie eine Umgebung für die Arbeit mit Postgres.
2. Melden Sie sich als Benutzer *Postgres* an der *Postgres*-Datenbank an.
3. Erstellen Sie eine neue Postgres-Rolle (in diesem Beispiel heißt die Rolle *KSCAdmin*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<password>';
   ```

4. Erstellen Sie eine Datenbank für den Administrationsserver (in diesem Beispiel ist der Name dieser Datenbank *KAV*):

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   Wenn die Fehlermeldung "New encoding (UTF8) is incompatible with the encoding of the template database" erscheint, erstellen Sie eine Datenbank mit dem Befehl:
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   Anstelle des Befehls:
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. Gewähren Sie der Rolle alle Berechtigungen für die Administrationsserver-Datenbank.

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   Stellen Sie sicher, dass die Rolle über die standardmäßigen Privilegien CONNECT und TEMPORARY für die Administrationsserver-Datenbank verfügt.

6. Gewähren Sie der erstellten Postgres-Rolle die folgenden Privilegien:

   - Privilegien für alle Tabellen im Schema "public": ALL
   - Berechtigungen für alle Sequenzen im Schema "public": ALL

   Melden Sie sich dazu als Benutzer *Postgres* an der Serverdatenbank an und führen Sie anschließend das folgende Skript aus (in diesem Skript lautet die Rolle *KSCAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. Melden Sie sich beim System unter dem Windows-Konto an, das zum Ausführen des Installationsprogramms verwendet wurde.

8. Führen Sie das Installationsprogramm des Administrationsservers aus.

   Der Installationsassistent zum Einrichten des Administrationsservers wird gestartet. Folgen Sie den Anweisungen des Assistenten.

9. Wählen Sie die Option Benutzerdefinierte Installation des Administrationsservers aus.

10. Wählen Sie PostgreSQL oder Postgres Pro als DBMS aus, in dem die Administrationsserver-Datenbank gespeichert wird.

11. Geben Sie den Namen der Serverdatenbank an. Verwenden Sie denselben Datenbanknamen, den Sie im Skript angeben. Beachten Sie, dass beim Datenbanknamen zwischen Groß- und Kleinschreibung unterschieden wird.

12. Geben Sie die Anmeldeinformationen der Postgres-Rolle an.

13. Geben Sie das Windows-Konto an, das zum Starten des Dienstes des Administrationsservers verwendet wird.

    Sie können ein vorhandenes Windows-Benutzerkonto auswählen oder mithilfe des Installers automatisch ein neues Windows-Konto im "KL-AK-*"-Format erstellen. Unabhängig von der Kontoauswahl weist der Installer dem Dienstkonto des Administrationsservers die erforderlichen Systemrechte zu.

Nach Abschluss der Installation verwendet der Administrationsserver die erstellte Datenbank zum Speichern der Daten des Administrationsservers. Der Administrationsserver ist einsatzbereit.

Szenario: Authentifizierung von Microsoft SQL Server

Die Informationen in diesem Abschnitt gelten nur für Konfigurationen, in denen von Kaspersky Security Center ein Microsoft SQL Server als Datenbankverwaltungssystem verwendet wird.

Um die von Kaspersky Security Center in die oder aus der Datenbank übertragenen Daten, sowie die in der Datenbank gespeicherten Daten, vor unbefugtem Zugriff zu schützen, müssen Sie die Kommunikation zwischen Kaspersky Security Center und SQL Server sichern. Die zuverlässigste Möglichkeit zur Bereitstellung einer sicheren Kommunikation besteht darin, Kaspersky Security Center und SQL Server auf demselben Gerät zu installieren und den Mechanismus für gemeinsame Speichernutzung für beide Anwendungen zu verwenden. In allen anderen Fällen empfehlen wir die Verwendung eines SSL- oder TLS-Zertifikats zur Authentifizierung der SQL Server-Instanz. Sie können ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (certificate authority - CA) oder ein selbstsigniertes Zertifikat verwenden. Wir empfehlen jedoch, ein Zertifikat einer vertrauenswürdigen CA zu verwenden, da ein selbstsigniertes Zertifikat nur einen begrenzten Schutz bietet.

Die Authentifizierung des SQL Servers erfolgt schrittweise:

1. **Generieren eines selbstsignierten SSL- oder TLS-Zertifikats für SQL Server gemäß den Zertifikatanforderungen**

   Wenn Sie bereits ein Zertifikat für SQL Server haben, überspringen Sie diesen Schritt.

   Ein SSL-Zertifikat gilt nur für Versionen von SQL Server vor 2016 (13.x). Verwenden Sie für SQL Server 2016 (13.x) und spätere Versionen ein TLS-Zertifikat.

   Geben Sie beispielsweise zum Generieren eines TLS-Zertifikats den folgenden Befehl in PowerShell ein:

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

Im Befehl müssen Sie Anstelle von "SQL_HOST_NAME" den Hostnamen des SQL Servers eingeben, wenn der Host in der Domäne enthalten ist, oder den *vollqualifizierten Domänennamen* (FQDN) des Hosts, wenn der Host nicht in der Domäne enthalten ist. Der gleiche Name - Hostname oder FQDN - muss im Installationsassistent des Administrationsservers als Instanzname des SQL Servers angegeben werden.

2. **Hinzufügen des Zertifikats zur SQL Server-Instanz**

   Die Anweisungen für diesen Schritt hängen von der Plattform ab, auf der SQL Server ausgeführt wird. Weitere Informationen finden Sie in der offiziellen Dokumentation:

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   Um das Zertifikat in einem Hochverfügbarkeitscluster zu verwenden, müssen Sie das Zertifikat auf jedem Knoten des Hochverfügbarkeitsclusters installieren. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

3. **Zuweisen der Berechtigungen des Dienstkontos**

   Stellen Sie sicher, dass das Dienstkonto, unter dem der Dienst des SQL Servers ausgeführt wird, über die vollen Berechtigungen für den Zugriff auf private Schlüssel verfügt. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

4. **Hinzufügen des Zertifikats zur Liste der vertrauenswürdigen Zertifikate für Kaspersky Security Center**

   Fügen Sie auf dem Administrationsserver-Gerät das Zertifikat zur Liste der vertrauenswürdigen Zertifikate hinzu. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

5. **Aktivieren verschlüsselter Verbindungen zwischen der SQL Server-Instanz und Kaspersky Security Center**

   Setzen Sie auf dem Administrationsserver-Gerät den Wert der Umgebungsvariable `KLDBADO_UseEncryption` auf `1`. Beispielsweise können Sie in Windows Server 2012 R2 die Umgebungsvariablen ändern, indem Sie auf der Registerkarte **Erweitert** des Fensters **Systemeigenschaften** auf **Umgebungsvariablen** klicken. Fügen Sie eine neue Variable namens `KLDBADO_UseEncryption` hinzu und setzen Sie ihren Wert auf `1`.

6. **Zusätzliche Konfiguration für die Verwendung des TLS 1.2-Protokolls**

   Wenn Sie das TLS 1.2-Protokoll verwenden, gehen Sie zusätzlich wie folgt vor:

   - Stellen Sie sicher, dass die installierte Version von SQL Server eine 64-Bit-Anwendung ist.
   - Installieren Sie den Microsoft OLE DB-Treiber auf dem Gerät mit dem Administrationsserver. Weitere Informationen finden Sie in der Dokumentation von Microsoft.
   - Setzen Sie auf dem Gerät mit dem Administrationsserver den Wert der Umgebungsvariable `KLDBADO_UseMSOLEDBSQL` auf `1`. Beispielsweise können Sie in Windows Server 2012 R2 die Umgebungsvariablen ändern, indem Sie auf der Registerkarte **Erweitert** des Fensters **Systemeigenschaften** auf **Umgebungsvariablen** klicken. Fügen Sie eine neue Variable namens `KLDBADO_UseMSOLEDBSQL` hinzu und setzen Sie ihren Wert auf `1`.

     Wenn die OLE DB-Treiberversion 19 oder neuer ist, geben Sie auch für die Umgebungsvariable `KLDBADO_ProviderName` den Wert `MSOLEDBSQL19` an.

7. **Aktivieren der Verwendung des TCP/IP-Protokolls auf einer benannten Instanz von SQL Server**

   Wenn Sie eine benannte Instanz eines SQL Servers verwenden, müssen Sie zusätzlich die Verwendung des TCP/IP-Protokolls aktivieren und der Databank-Engine des SQL Servers eine TCP/IP-Portnummer zuweisen. Wenn Sie die SQL Server-Verbindung im Installationsassistenten des Administrationsservers konfigurieren, geben Sie den Hostnamen und die Portnummer des SQL Servers im Feld **Name der SQL Server-Instanz** an.

Szenario: Authentifizierung am MySQL-Server

Es wird empfohlen, für die Authentifizierung am MySQL-Servers ein TLS-Zertifikat zu verwenden. Sie können ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (certificate authority - CA) oder ein selbstsigniertes Zertifikat verwenden.

Der Administrationsserver unterstützt für MySQL sowohl die unidirektionale als auch die bidirektionale SSL-Authentifizierung.

Aktivieren der unidirektionalen SSL-Authentifizierung

Gehen Sie folgendermaßen vor, um die unidirektionale SSL-Authentifizierung für MySQL zu konfigurieren:

1. **Generieren Sie ein selbstsigniertes TLS-Zertifikat für den MySQL-Server**

   Starten Sie die PowerShell und wechseln Sie in den Ordner, in dem Sie die Zertifikate speichern möchten. Führen Sie die folgenden Befehle aus:

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

   Diese Befehle erstellen Zertifikate für den aktuellen Benutzer und exportieren die Zertifikate in das PEM-Format. Zur Authentifizierung des Servers benötigen nur die exportierten PEM-Dateien. Um die erstellten Zertifikate in Windows zu löschen, führen Sie den folgenden Befehl in der PowerShell aus:

```
certmgr.msc
```

   Suchen Sie die erstellten Zertifikate im Ordner **Persönlich** → **Zertifikate** und löschen Sie diese.

2. **Erstellen Sie eine Server-Flag-Datei**

Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

Verwenden Sie das Tool "klscflag", um das Server-Flag KLSRV_MYSQL_OPT_SSL_CA zu erstellen, und geben Sie den Pfad des Zertifikats als dessen Wert an.

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <Pfad zu ca-cert.pem> -t s
```

3. **Konfigurieren Sie die Datenbank**

   Geben Sie die Zertifikate in der Datei "my.cnf" an. Öffnen Sie die Datei "my.cnf" in einem Texteditor und fügen Sie im Abschnitt "[mysqld]" die folgenden Zeilen hinzu:

   ```
   [mysqld]
   ssl-ca="...\mysqlcerts\ca-cert.pem"
   ssl-cert="...\mysqlcerts\server-cert.pem"
   ssl-key="...\mysqlcerts\server-key.pem"
   ```

Aktivieren der bidirektionalen SSL-Authentifizierung

Gehen Sie folgendermaßen vor, um die bidirektionale SSL-Authentifizierung für MySQL zu konfigurieren:

1. **Erstellen Sie Server-Flag-Dateien**

   Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

   Verwenden Sie das Tool "klscflag", um die Server-Flags zu erstellen, und geben Sie die Pfade der Zertifikate als deren Wert an.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <Pfad zu ca-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <Pfad zu server-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <Pfad zu server-key.pem> -t s
   ```

2. **Geben Sie die Passphrase an (optional)**

   Wenn server-key.pem eine Passphrase erfordert, erstellen Sie das Flag KLSRV_MARIADB_OPT_TLS_PASPHRASE und geben Sie die Passphrase als dessen Wert an:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <Passphrase> -t s
   ```

3. **Konfigurieren Sie die Datenbank**

   Geben Sie die Zertifikate in der Datei "my.cnf" an. Öffnen Sie die Datei "my.cnf" in einem Texteditor und fügen Sie im Abschnitt "[mysqld]" die folgenden Zeilen hinzu:

   ```
   [mysqld]
   ssl-ca="...\ca-cert.pem"
   ssl-cert="...\server-cert.pem"
   ssl-key="...\server-key.pem"
   ```

Szenario: Authentifizierung am PostgreSQL-Server

Es wird empfohlen, für die Authentifizierung am PostgreSQL-Server ein TLS-Zertifikat zu verwenden. Sie können ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (certificate authority - CA) oder ein selbstsigniertes Zertifikat verwenden. Verwenden Sie ein Zertifikat einer vertrauenswürdigen CA, da ein selbstsigniertes Zertifikat nur einen begrenzten Schutz bietet.

Der Administrationsserver unterstützt für PostgreSQL sowohl die unidirektionale als auch die bidirektionale SSL-Authentifizierung.

Die Authentifizierung von PostgreSQL Server erfolgt schrittweise:

1. **Generieren eines Zertifikats für den PostgreSQL-Server**

   Führen Sie in einem OpenSSL-basierten Cross-Plattform-Tool die folgenden Befehle aus:

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj
   "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **Generieren eines Zertifikats für den Administrationsserver**

   Führen Sie die folgenden Befehle aus. Der CN-Wert sollte mit dem Namen des Benutzers übereinstimmen, der sich im Namen des Administrationsservers mit PostgreSQL verbindet. Der Benutzername ist standardmäßig auf "postgres" eingestellt.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -
   subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **Konfigurieren der Authentifizierung des Client-Zertifikats**

   Ändern Sie die Datei "pg_hba.conf" wie folgt:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   Stellen Sie sicher, dass die Datei "pg_hba.conf" keinen Eintrag enthält, der mit `host` beginnt.

4. **Angeben des PostgreSQL-Zertifikats**

   Für die unidirektionale SSL-Authentifizierung

   Ändern Sie die Datei "postgresql.conf" wie folgt (geben Sie den korrekten Pfad zu den crt- und key-Dateien an):

   ```
   listen_addresses ='localhost, server-ip'
   ```

   ```
   ssl = on
   ```

   ```
   ssl_cert_file = '<psql.crt>'
   ```

   ```
   ssl_key_file = '<psql.key>'
   ```

   Für die bidirektionale SSL-Authentifizierung

   Ändern Sie die Datei "postgresql.conf" wie folgt (geben Sie die korrekten Pfade zu den crt- und key-Dateien an):

   ```
   listen_addresses ='localhost, server-ip'
   ```

   ```
   ssl = on
   ```

```
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **Neustarten des PostgreSQL-Daemons**

   Führen Sie den folgenden Befehl aus:

   ```
   systemctl restart postgresql-14.service
   ```

6. **Angeben des Server-Flags für den Administrationsserver.**

   Für die unidirektionale SSL-Authentifizierung

   Verwenden Sie das Tool "klscflag", um das Server-Flag KLSRV_POSTGRES_OPT_SSL_CA zu erstellen, und geben Sie den Pfad des Zertifikats als dessen Wert an.

   Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

   Führen Sie den folgenden Befehl aus:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <Pfad zu psql.crt> -t s
   ```

   Für die bidirektionale SSL-Authentifizierung

   Verwenden Sie das Tool "klscflag", um die Server-Flags zu erstellen, und geben Sie die Pfade der Zertifikate als deren Wert an.

   Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

   Führen Sie die folgenden Befehle aus:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <Pfad zu psql.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <Pfad zu postgres.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <Pfad zu postgres.key> -t s
   ```

   Wenn `postgres.key` eine Passphrase erfordert, erstellen Sie das Flag KLSRV_POSTGRES_OPT_TLS_PASPHRASE und geben Sie die Passphrase als dessen Wert an:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <Passphrase> -t s
   ```

7. **Neustarten des Dienstes des Administrationsservers**

Installationsempfehlungen für den Administrationsserver

Dieser Abschnitt enthält Empfehlungen in Bezug auf die Installation des Administrationsservers. Im Abschnitt finden Sie ferner Szenarien für die Nutzung des freigegebenen Ordners auf dem Gerät mit dem Administrationsserver zur Bereitstellung des Administrationsagenten auf den Client-Geräten.

Benutzerkonten für die Dienste des Administrationsservers auf dem Failover-Cluster erstellen

Standardmäßig erstellt der Installer selbständig keine nicht privilegierten Benutzerkonten für die Dienste des Administrationsservers. Dieses Verhalten eignet sich am besten für die Installation des Administrationsservers auf einem gewöhnlichen Gerät.

Bei der Installation des Administrationsservers auf einem störungssicheren Cluster muss jedoch anders vorgegangen werden:

1. Die nicht privilegierten Domänenbenutzerkonten für die Dienste des Administrationsservers erstellen und zu Mitgliedern der globalen Domänensicherheitsgruppe KLAdmins machen.

2. Im Installer des Administrationsservers die erstellten Domänenbenutzerkonten für Dienste festlegen.

Den freigegebenen Ordner angeben

Bei der Installation des Administrationsservers kann der Ort des freigegebenen Ordners festgelegt werden. Sie können ferner den Ort des freigegebenen Ordners nach der Installation in den Eigenschaften des Administrationsservers angeben. Standardmäßig wird der freigegebene Ordner auf dem Gerät mit dem Administrationsserver (mit Lesezugriff für die integrierte Gruppe **Everyone**) erstellt. In einigen Fällen (wie hohe Belastung oder die Notwendigkeit des Zugriffes aus einem isolierten Netzwerk) ist es jedoch zweckmäßig, den freigegebenen Ordner auf einer speziellen Dateiressource zu erstellen.

Der freigegebene Ordner wird in einigen Szenarien der Bereitstellung des Administrationsagenten verwendet.

Die Unterscheidung von Groß- und Kleinschreibung muss deaktiviert sein.

Remote-Installation über den Administrationsserver mithilfe von Gruppenrichtlinien des Active Directory

Falls sich die Geräte in der Windows-Domäne befinden (ohne Arbeitsgruppen), ist es zweckmäßig, die erstmalige Bereitstellung (Installation des Administrationsagenten und der Sicherheitsanwendungen auf bisher noch nicht verwalteten Geräte) mithilfe der Gruppenrichtlinien von Active Directory auszuführen. Die Bereitstellung wird mithilfe der Standardaufgabe zur Remote-Installation von Kaspersky Security Center ausgeführt. Wenn das Netzwerk sehr groß ist, kann es zweckmäßig sein, zwecks der Verkleinerung der Belastung des Laufwerksubsystems des Geräts mit dem Administrationsserver den gemeinsamen Ordner auf einer speziellen Dateiressource zu erstellen.

Remote-Installation über den Versand des UNC-Pfads an das autonome Paket

Falls die Benutzer der Geräte im Unternehmensnetzwerk über die Berechtigungen eines lokalen Administrators verfügen, besteht eine weitere Methode zur erstmaligen Bereitstellung im Erstellen eines autonomen Pakets des Administrationsagenten (oder sogar eines "Doppelpakets" von Administrationsagent und Sicherheitsanwendung). Nach dem Erstellen des autonomen Paketes muss an die Benutzer der Geräte des Netzwerkes ein Link auf das Paket gesendet werden, das sich im freigegebenen Ordner befindet. Die Installation wird über den Link ausgeführt.

Update aus dem freigegebenen Ordner des Administrationsservers

In der Update-Aufgabe von Anti-Virus kann das Update aus dem freigegebenen Ordner des Administrationsservers angepasst werden. Wenn die Aufgabe einer großen Anzahl der Geräte zugewiesen ist, ist es zweckmäßig, den freigegebenen Ordner auf einer speziellen Dateiressource zu erstellen.

Betriebssystem-Images installieren

Die Installation von Betriebssystem-Images wird immer unter Nutzung des freigegebenen Ordners ausgeführt: die Geräte lesen die Betriebssystem-Images aus dem Ordner aus. Wenn die Bereitstellung der Images für eine große Anzahl der Geräte des Unternehmens geplant wird, ist es zweckmäßig, den freigegebenen Ordner auf einer speziellen Dateiressource zu erstellen.

Adresse des Administrationsservers angeben

Bei der Installation des Administrationsservers kann die Adresse des Administrationsservers festgelegt werden. Diese Adresse wird standardmäßig beim Erstellen der Installationspakete des Administrationsagenten verwendet.

Als Adresse des Administrationsservers können Sie Folgendes angeben:

- NetBIOS-Name des Administrationsservers, der standardmäßig angegeben ist
- Vollqualifizierter Domänenname (FQDN) des Administrationsservers, wenn das Domain Name System (DNS) im Netzwerk der Organisation konfiguriert wurde und ordnungsgemäß funktioniert
- Externe Adresse, wenn der Administrationsserver in der demilitarisierten Zone (DMZ) installiert ist

In Folge kann die Adresse des Administrationsservers mithilfe der Verwaltungskonsole geändert werden, dabei wird er jedoch wird nicht automatisch in den schon erstellten Installationspaketen des Administrationsagenten geändert.

Standardinstallation

Die Standardinstallation ist eine Installation des Administrationsservers, bei der Standardpfade zu Programmdateien verwendet werden, ein Standardset an Plug-ins installiert wird und die Komponente "Verwaltung mobiler Geräte" nicht aktiviert wird.

Um Kaspersky Security Center Administrationsserver auf einem lokalen Gerät zu installieren,

Starten Sie die ausführbare Datei "ksc_<Versionsnummer>.<Buildnummer>_full_<Sprache der Lokalisierung>.exe".

Ein Fenster wird geöffnet, in dem Sie Kaspersky-Anwendungen zur Installation auswählen können. Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

Schritt 1. Anzeigen des Lizenzvertrags und der Datenschutzrichtlinie

Machen Sie sich in diesem Schritt des Installationsassistenten mit dem Lizenzvertrag vertraut, den Sie mit Kaspersky abschließen, sowie mit der Datenschutzrichtlinie.

Außerdem werden Sie eventuell aufgefordert, sich mit den Lizenzverträgen und Datenschutzrichtlinien für die im Programmpaket von Kaspersky Security Center verfügbaren Plug-ins für die Programmverwaltung vertraut zu machen.

Bitte lesen Sie sorgfältig den Lizenzvertrag und die Datenschutzrichtlinie. Wenn Sie mit allen Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, bestätigen Sie dies durch das Aktivieren der entsprechenden Kontrollkästchen.

Die Programminstallation wird nach dem Aktivieren beider Kontrollkästchen fortgesetzt.

Falls Sie dem Lizenzvertrag oder der Datenschutzrichtlinie nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

Schritt 2. Installationsart auswählen

Geben Sie im Auswahlfenster für den Installationstyp den Typ **Standard** an.

Die Standardinstallation wird empfohlen, wenn Sie sich mit Kaspersky Security Center bekannt machen und die Ausführung des Programms z. B. in einem kleinen Bereich des Unternehmensnetzwerks testen möchten. Bei der Standardinstallation passen Sie nur die Einstellungen der Datenbank an. Die Einstellungen des Administrationsservers werden nicht angepasst; für sie werden die festgelegten Standardwerte verwendet. Die Standardinstallation erlaubt nicht die Auswahl der zu installierenden Verwaltungs-Plug-ins; es wird ein Standardset an Plug-ins installiert. Während einer Standardinstallation werden keine Installationspakete für mobile Geräte erstellt. Sie können Sie jedoch später in der Verwaltungskonsole erstellen.

Schritt 3. Kaspersky Security Center Web Console installieren

Dieser Schritt wird nur angezeigt, wenn Sie ein 64-Bit-Betriebssystem verwenden. Andernfalls wird dieser Schritt nicht angezeigt, da Kaspersky Security Center Web Console keine 32-Bit-Betriebssysteme unterstützt.

Standardmäßig werden sowohl Kaspersky Security Center Web Console als auch die MMC-basierte Verwaltungskonsole installiert.

Wenn Sie nur Kaspersky Security Center Web Console installieren möchten:

1. Wählen Sie **Nur diese installieren**.
2. Wählen Sie in der Dropdown-Liste **Webbasierte Konsole**.

Die Installation von Kaspersky Security Center Web Console wird automatisch gestartet, nachdem die Administrationsserver-Installation abgeschlossen wurde.

Wenn Sie nur die MMC-basierte Verwaltungskonsole installieren möchten:

1. Wählen Sie **Nur diese installieren**.
2. Wählen Sie in der Dropdown-Liste **MMC-basierte Konsole**.

Schritt 4. Auswählen der Netzwerkgröße

Geben Sie die Größe des Netzwerks an, in dem Kaspersky Security Center installiert werden soll. Der Assistent berücksichtigt die Anzahl der Geräte im Netzwerk und passt die Installationseinstellungen und die Darstellung der Programmoberfläche dementsprechend an.

In der Tabelle unten sind die Installationseinstellungen für das Programm und die Darstellung der Programmoberfläche bei Auswahl von verschiedenen Netzwerkgrößen aufgeführt.

Installationseinstellungen je nach Netzwerkgröße

Einstellungen	1 – 100 verwaltete Geräte	101 – 1.000 verwaltete Geräte	1.001 – 5.000 verwaltete Geräte	Mehr als 5.000 verwaltete Geräte
Mit dem Knoten des sekundären und virtuellen Administrationsservers, sowie mit allen Einstellungen, die für sekundäre und virtuelle Administrationsserver relevant sind, in der Konsolenstruktur anzeigen (nur in der MMC-basierten Verwaltungskonsole verfügbar)	Nicht vorhanden	Nicht vorhanden	Vorhanden	Vorhanden
Mit den Abschnitten **Sicherheit** in den Eigenschaftsfenstern des Administrationsservers und der Administrationsgruppen anzeigen (nur in der MMC-basierten Verwaltungskonsole verfügbar)	Nicht vorhanden	Nicht vorhanden	Vorhanden	Vorhanden
Zufällige Verteilung der Startzeit für die Update-Aufgabe auf Client-Geräten	Nicht vorhanden	im Abstand von 5 Minuten	im Abstand von 10 Minuten	im Abstand von 10 Minuten

Falls Sie den Administrationsserver mit einem MySQL 5.7, oder SQL Express-Datenbankserver verbinden, wird es nicht empfohlen, das Programm zur Verwaltung von mehr als 10.000 Geräten zu verwenden. Für das MariaDB-DBMS beträgt die empfohlene maximale Anzahl verwalteter Geräte 20.000 Stück.

Schritt 5. Auswählen der Datenbank

Wählen Sie in diesem Schritt des Assistenten eins der folgenden Datenbankverwaltungssysteme (DBMS) aus, welches zum Speichern der Administrationsserver-Datenbank verwendet wird:

- **Microsoft SQL Server oder SQL Server Express**
- **MySQL oder MariaDB**
- **PostgreSQL oder Postgres Pro**

Es wird empfohlen, den Administrationsserver anstatt auf einem Domänencontroller auf einem dezidierten Server zu installieren. Wenn Sie Kaspersky Security Center jedoch auf einem Server installieren, der als schreibgeschützter Domänencontroller (RODC) agiert, muss Microsoft SQL Server (SQL Express) nicht lokal (auf demselben Gerät) installiert werden. In diesem Fall empfehlen wir Ihnen, Microsoft SQL Server (SQL Express) per Fernzugriff (auf einem anderen Gerät) zu installieren, oder MySQL, MariaDB oder PostgreSQL zu verwenden, falls Sie das DBMS lokal installieren müssen.

Die Datenbankstruktur des Administrationsservers ist in der Datei klakdb.chm enthalten, die sich im Installationsordner von Kaspersky Security Center befindet. Diese Datei ist auch als Archiv auf dem Kaspersky-Portal verfügbar: klakdb.zip.

Schritt 6. Konfigurieren des SQL-Servers

Geben Sie in diesem Schritt des Assistenten je nach ausgewähltem Datenbankverwaltungssystem (DBMS) die folgenden Verbindungseinstellungen an:

- Wenn Sie im vorherigen Schritt **Microsoft SQL Server oder SQL Server Express** ausgewählt haben:

  - Geben Sie im Feld **Name der SQL Server-Instanz** den Namen des SQL-Servers an, der im Netzwerk installiert ist. Mit der Schaltfläche **Durchsuchen** kann die Liste aller im Netzwerk installierten SQL-Server angezeigt werden. Standardmäßig ist dieses Feld leer.

    Wenn Sie eine Verbindung über einen benutzerdefinierten Port zum SQL Server herstellen, geben Sie den Hostnamen des SQL Servers zusammen mit der durch ein Komma getrennten Portnummer an, z. B.:

    ```
    SQL_Server_host_name,1433
    ```

    Wenn Sie die Kommunikation zwischen dem Administrationsserver und SQL Server mittels eines Zertifikats absichern, geben Sie im Feld **Name der SQL Server-Instanz** denselben Hostnamen an, der beim Generieren des Zertifikats verwendet wurde. Wenn Sie eine benannte Instanz von SQL Server verwenden, geben Sie den Hostnamen des SQL-Servers zusammen mit der durch ein Komma getrennten Portnummer an, z. B.:

    ```
    SQL_Server_name,1433
    ```

    Wenn Sie mehrere Instanzen von SQL-Servern auf demselben Host verwenden, geben Sie zusätzlich den durch einen Backslash getrennten Instanznamen an, z. B.:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Wenn auf einem SQL Server im Unternehmensnetzwerk die Always-On-Funktion aktiviert ist, geben Sie den Namen des Verfügbarkeitsgruppenlisteners im Feld **Name der SQL Server-Instanz** an. Beachten Sie, dass der Administrationsserver den Verfügbarkeitsmodus für synchrone Commits nur unterstützt, wenn die Always-On-Funktion aktiviert ist.

  - Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

  Wenn Sie auf diesem Schritt einen SQL-Server manuell auf demselben Gerät installieren möchten, von dem aus die Installation von Kaspersky Security Center erfolgt, müssen Sie die Installation abbrechen und sie nach der Installation des SQL-Servers erneut starten. Die unterstützten SQL-Server werden in den Systemanforderungen aufgezählt.

  Wenn Sie einen SQL-Server auf einem Remote-Gerät installieren wollen, muss der Installationsassistent für Kaspersky Security Center nicht abgebrochen werden. Installieren Sie den SQL-Server, und fahren Sie mit der Installation von Kaspersky Security Center fort.

- Wenn Sie im vorherigen Schritt **MySQL oder MariaDB** ausgewählt haben:

  - Geben Sie im Feld **Name der SQL Server-Instanz** den Namen der DBMS-Instanz an. Standardmäßig wird die IP-Adresse des Geräts verwendet, auf dem Kaspersky Security Center installiert wird.

  - Geben Sie im Feld **Port** den Port für die Verbindung des Administrationsservers mit dem DBMS an. Standardmäßig wird Portnummer 3306 verwendet.

  - Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

- Wenn Sie im vorherigen Schritt **PostgreSQL oder Postgres Pro** ausgewählt haben:

  - Geben Sie im Feld **PostgreSQL- oder Postgres Pro-Server** den Namen der DBMS-Instanz an. Standardmäßig wird die IP-Adresse des Geräts verwendet, auf dem Kaspersky Security Center installiert wird.

  - Geben Sie im Feld **Port** den Port für die Verbindung des Administrationsservers mit dem DBMS an. Standardmäßig wird Portnummer 5432 verwendet.

  - Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

Schritt 7. Auswählen eines Authentifizierungsmodus

Legen Sie den Authentifizierungsmodus fest, der beim Verbindungsaufbau des Administrationsservers mit dem Datenbankmanagementsystem (DBMS) verwendet werden soll.

In Abhängigkeit vom ausgewählten DBMS können Sie von den folgenden Authentifizierungsmodi auswählen:

- Wählen Sie für SQL Express oder Microsoft SQL Server eine der folgenden Varianten aus:

  - **Microsoft-Windows-Authentifizierungsmodus**. In diesem Fall wird beim Überprüfen der Berechtigungen das Benutzerkonto für den Start des Administrationsservers herangezogen.

  - **SQL Server-Authentifizierungsmodus**. Bei dieser Variante wird für die Überprüfung der Berechtigungen das im Fenster angegebene Benutzerkonto herangezogen. Fülle Sie die Felder **Benutzerkonto** und **Kennwort** aus.

    Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen**.

  Für beide Authentifizierungsmodi untersucht die Anwendung, ob die Datenbank verfügbar ist. Wenn die Datenbank nicht verfügbar ist, wird eine Fehlermeldung angezeigt und Sie müssen die korrekten Anmeldedaten angeben.

  Wenn sich die Administrationsserver-Datenbank auf einem anderen Gerät befindet und das Benutzerkonto des Administrationsservers keinen Zugriff auf den Datenbankserver hat, muss bei der Installation oder dem Update des Administrationsservers die Authentifizierung des SQL-Servers verwendet werden. Dieser Fall kann eintreten, wenn sich das Gerät mit der Datenbank nicht in der Domäne befindet oder der Administrationsserver unter dem Konto "LocalSystem" installiert wurde.

- Geben Sie für MySQL, MariaDB, PostgreSQL oder Postgres Pro das Konto und das Passwort an.

Schritt 8. Entpacken und Installieren der Dateien auf der Festplatte

Nach der Konfiguration der Installationseinstellungen für die Komponenten von Kaspersky Security Center können Sie die Installation auf der Festplatte starten.

Wenn zusätzliche Programme für den Start der Installation erforderlich sind, meldet dies der Installationsassistent vor der Installation von Kaspersky Security Center auf der Seite **Installation der Pflichtkomponenten**. Die erforderlichen Programme werden automatisch nach dem Klicken auf die Schaltfläche **Weiter** installiert.

Auf der letzten Seite können Sie auswählen, welche Konsole für die Arbeit mit Kaspersky Security Center gestartet werden soll:

- **MMC-basierte Verwaltungskonsole starten**
- **Kaspersky Security Center Web Console starten**

  Diese Option ist nur verfügbar, wenn Sie in einem der vorherigen Schritte Kaspersky Security Center Web Console installiert haben.

Sie können außerdem auf **Fertigstellen** klicken, um den Assistenten abzuschließen, ohne Kaspersky Security Center zu verwenden. Sie können später jederzeit mit der Verwendung des Programms beginnen.

Beim ersten Start der Verwaltungskonsole oder Kaspersky Security Center Web Console können Sie eine Erstkonfiguration des Programms ausführen.

Nach Abschluss des Installationsassistenten werden die folgenden Programmkomponenten auf der Festplatte installiert, auf welcher das Betriebssystem installiert wurde:

- Administrationsserver (zusammen mit Serverversion des Administrationsagenten)
- Verwaltungskonsole auf Basis der Microsoft Management Console
- Kaspersky Security Center Web Console (falls Sie diese installieren)
- Alle im Programmpaket verfügbaren Plug-ins für die Programmverwaltung

Außerdem wird das Programm Microsoft Windows Installer Version 4.5 installiert, falls es nicht bereits installiert ist.

Benutzerdefinierte Installation

Die benutzerdefinierte Installation ist eine Installationsart des Administrationsservers, bei der Sie die Komponenten für die Installation auswählen und den Ordner angeben können, in dem das Programm installiert werden soll.

Mit Hilfe dieses Installationstyps können Sie die Einstellungen der Datenbank, die Einstellungen des Administrationsservers konfigurieren und die Komponenten installieren, die nicht Teil der Standardinstallation und der Verwaltungs-Plug-ins für die Sicherheitsanwendungen von Kaspersky sind. Sie können ferner die Komponente "Verwaltung mobiler Geräte" aktivieren.

Um Kaspersky Security Center Administrationsserver auf einem lokalen Gerät zu installieren,

Starten Sie die ausführbare Datei "ksc_<Versionsnummer>.<Buildnummer>_full_<Sprache der Lokalisierung>.exe".

Ein Fenster wird geöffnet, in dem Sie Kaspersky-Anwendungen zur Installation auswählen können. Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

Schritt 1. Anzeigen des Lizenzvertrags und der Datenschutzrichtlinie

Machen Sie sich in diesem Schritt des Installationsassistenten mit dem Lizenzvertrag vertraut, den Sie mit Kaspersky abschließen, sowie mit der Datenschutzrichtlinie.

Außerdem werden Sie eventuell aufgefordert, sich mit den Lizenzverträgen und Datenschutzrichtlinien für die im Programmpaket von Kaspersky Security Center verfügbaren Plug-ins für die Programmverwaltung vertraut zu machen.

Bitte lesen Sie sorgfältig den Lizenzvertrag und die Datenschutzrichtlinie. Wenn Sie mit allen Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, bestätigen Sie dies durch das Aktivieren der entsprechenden Kontrollkästchen.

Die Programminstallation wird nach dem Aktivieren beider Kontrollkästchen fortgesetzt.

Falls Sie dem Lizenzvertrag oder der Datenschutzrichtlinie nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

Schritt 2. Installationsart auswählen

Geben Sie im Auswahlfenster für den Installationstyp den Typ **Benutzerdefiniert** an.

Die benutzerdefinierte Installation erlaubt das Ändern bestimmter Einstellungen von Kaspersky Security Center wie z. B. den Pfad zum gemeinsamen Ordner, Benutzerkonten und Ports für die Verbindung mit dem Administrationsserver sowie die Einstellungen der Datenbank. Bei der benutzerdefinierten Installation können Sie angeben, welche Verwaltungs-Plug-ins für Programme von Kaspersky installiert werden sollen. Bei der benutzerdefinierten Installation können Sie Installationspakete für mobile Geräte erstellen, indem Sie die entsprechende Option auswählen.

Schritt 3. Auswählen der zu installierenden Komponenten

Wählen Sie die Komponenten des Kaspersky Security Center Administrationsservers aus, die installiert werden sollen:

- **Verwaltung mobiler Geräte**. Aktivieren Sie dieses Kontrollkästchen, wenn während der Ausführung des Installationsassistenten von Kaspersky Security Center Installationspakete für mobile Geräte erstellt werden sollen. Sie können die Installationspakete für mobile Geräte nach der Installation des Administrationsservers auch manuell über die Verwaltungskonsole erstellen.

- **SNMP-Agent**. Empfängt statistische Daten für den Administrationsserver mit dem SNMP-Protokoll. Die Komponente steht zur Verfügung, wenn bei der Installation des Programms auf dem Gerät die SNMP-Komponente installiert ist.

  Nach der Installation von Kaspersky Security Center befinden sich die für den Empfang von Statistikdaten benötigten mib-Dateien im Installationsverzeichnis im Unterordner SNMP.

Die Komponenten Administrationsagent und Verwaltungskonsole werden in der Liste der Komponenten nicht angezeigt. Diese Komponenten werden automatisch installiert und deren Installation kann nicht abgebrochen werden.

Geben Sie in diesem Schritt des Assistenten auch den Ordner für die Installation der Komponenten des Administrationsservers an. Standardmäßig werden die Komponenten in den Ordner <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center installiert. Wenn kein Ordner mit diesem Namen vorhanden ist, wird er automatisch während des Installationsvorgangs angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** ändern.

Schritt 4. Kaspersky Security Center Web Console installieren

Dieser Schritt wird nur angezeigt, wenn Sie ein 64-Bit-Betriebssystem verwenden. Andernfalls wird dieser Schritt nicht angezeigt, da Kaspersky Security Center Web Console keine 32-Bit-Betriebssysteme unterstützt.

Standardmäßig werden sowohl Kaspersky Security Center Web Console als auch die MMC-basierte Verwaltungskonsole installiert.

Wenn Sie nur Kaspersky Security Center Web Console installieren möchten:

1. Wählen Sie **Nur diese installieren**.
2. Wählen Sie in der Dropdown-Liste **Webbasierte Konsole**.

Die Installation von Kaspersky Security Center Web Console wird automatisch gestartet, nachdem die Administrationsserver-Installation abgeschlossen wurde.

Wenn Sie nur die MMC-basierte Verwaltungskonsole installieren möchten:

1. Wählen Sie **Nur diese installieren**.
2. Wählen Sie in der Dropdown-Liste **MMC-basierte Konsole**.

Schritt 5. Auswählen der Netzwerkgröße

Geben Sie die Größe des Netzwerks an, in dem Kaspersky Security Center installiert werden soll. Der Assistent berücksichtigt die Anzahl der Geräte im Netzwerk und passt die Installationseinstellungen und die Darstellung der Programmoberfläche dementsprechend an.

In der Tabelle unten sind die Installationseinstellungen für das Programm und die Darstellung der Programmoberfläche bei Auswahl von verschiedenen Netzwerkgrößen aufgeführt.

Installationseinstellungen je nach Netzwerkgröße

Einstellungen	1 – 100 verwaltete Geräte	101 – 1.000 verwaltete Geräte	1.001 – 5.000 verwaltete Geräte	Mehr als 5.000 verwaltete Geräte
Mit dem Knoten des sekundären und virtuellen Administrationsservers, sowie mit allen Einstellungen, die für sekundäre und virtuelle Administrationsserver relevant sind, in der Konsolenstruktur anzeigen (nur in der MMC-basierten Verwaltungskonsole verfügbar)	Nicht vorhanden	Nicht vorhanden	Vorhanden	Vorhanden
Mit den Abschnitten **Sicherheit** in den Eigenschaftsfenstern des Administrationsservers und der Administrationsgruppen anzeigen (nur in der MMC-basierten Verwaltungskonsole verfügbar)	Nicht vorhanden	Nicht vorhanden	Vorhanden	Vorhanden
Zufällige Verteilung der Startzeit für die Update-Aufgabe auf Client-Geräten	Nicht vorhanden	im Abstand von 5 Minuten	im Abstand von 10 Minuten	im Abstand von 10 Minuten

Falls Sie den Administrationsserver mit einem MySQL 5.7, oder SQL Express-Datenbankserver verbinden, wird es nicht empfohlen, das Programm zur Verwaltung von mehr als 10.000 Geräten zu verwenden. Für das MariaDB-DBMS beträgt die empfohlene maximale Anzahl verwalteter Geräte 20.000 Stück.

Schritt 6. Auswählen der Datenbank

Wählen Sie in diesem Schritt des Assistenten eins der folgenden Datenbankverwaltungssysteme (DBMS) aus, welches zum Speichern der Administrationsserver-Datenbank verwendet wird:

- **Microsoft SQL Server oder SQL Server Express**
- **MySQL oder MariaDB**
- **PostgreSQL oder Postgres Pro**

Es wird empfohlen, den Administrationsserver anstatt auf einem Domänencontroller auf einem dezidierten Server zu installieren. Wenn Sie Kaspersky Security Center jedoch auf einem Server installieren, der als schreibgeschützter Domänencontroller (RODC) agiert, muss Microsoft SQL Server (SQL Express) nicht lokal (auf demselben Gerät) installiert werden. In diesem Fall empfehlen wir Ihnen, Microsoft SQL Server (SQL Express) per Fernzugriff (auf einem anderen Gerät) zu installieren, oder MySQL, MariaDB oder PostgreSQL zu verwenden, falls Sie das DBMS lokal installieren müssen.

Die Datenbankstruktur des Administrationsservers ist in der Datei klakdb.chm enthalten, die sich im Installationsordner von Kaspersky Security Center befindet. Diese Datei ist auch als Archiv auf dem Kaspersky-Portal verfügbar: klakdb.zip.

Schritt 7. Konfigurieren des SQL-Servers

Geben Sie in diesem Schritt des Assistenten je nach ausgewähltem Datenbankverwaltungssystem (DBMS) die folgenden Verbindungseinstellungen an:

- Wenn Sie im vorherigen Schritt **Microsoft SQL Server oder SQL Server Express** ausgewählt haben:
  - Geben Sie im Feld **Name der SQL Server-Instanz** den Namen des SQL-Servers an, der im Netzwerk installiert ist. Mit der Schaltfläche **Durchsuchen** kann die Liste aller im Netzwerk installierten SQL-Server angezeigt werden. Standardmäßig ist dieses Feld leer.

Wenn Sie eine Verbindung über einen benutzerdefinierten Port zum SQL Server herstellen, geben Sie den Hostnamen des SQL Servers zusammen mit der durch ein Komma getrennten Portnummer an, z. B.:

```
SQL_Server_host_name,1433
```

Wenn Sie die Kommunikation zwischen dem Administrationsserver und SQL Server mittels eines Zertifikats absichern, geben Sie im Feld **Name der SQL Server-Instanz** denselben Hostnamen an, der beim Generieren des Zertifikats verwendet wurde. Wenn Sie eine benannte Instanz von SQL Server verwenden, geben Sie den Hostnamen des SQL-Servers zusammen mit der durch ein Komma getrennten Portnummer an, z. B.:

```
SQL_Server_name,1433
```

Wenn Sie mehrere Instanzen von SQL-Servern auf demselben Host verwenden, geben Sie zusätzlich den durch einen Backslash getrennten Instanznamen an, z. B.:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Wenn auf einem SQL Server im Unternehmensnetzwerk die Always-On-Funktion aktiviert ist, geben Sie den Namen des Verfügbarkeitsgruppenlisteners im Feld **Name der SQL Server-Instanz** an. Beachten Sie, dass der Administrationsserver den Verfügbarkeitsmodus für synchrone Commits nur unterstützt, wenn die Always-On-Funktion aktiviert ist.

- Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

Wenn Sie auf diesem Schritt einen SQL-Server manuell auf demselben Gerät installieren möchten, von dem aus die Installation von Kaspersky Security Center erfolgt, müssen Sie die Installation abbrechen und sie nach der Installation des SQL-Servers erneut starten. Die unterstützten SQL-Server werden in den Systemanforderungen aufgezählt.

Wenn Sie einen SQL-Server auf einem Remote-Gerät installieren wollen, muss der Installationsassistent für Kaspersky Security Center nicht abgebrochen werden. Installieren Sie den SQL-Server, und fahren Sie mit der Installation von Kaspersky Security Center fort.

- Wenn Sie im vorherigen Schritt **MySQL oder MariaDB** ausgewählt haben:

  - Geben Sie im Feld **Name der SQL Server-Instanz** den Namen der DBMS-Instanz an. Standardmäßig wird die IP-Adresse des Geräts verwendet, auf dem Kaspersky Security Center installiert wird.

  - Geben Sie im Feld **Port** den Port für die Verbindung des Administrationsservers mit dem DBMS an. Standardmäßig wird Portnummer 3306 verwendet.

  - Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

- Wenn Sie im vorherigen Schritt **PostgreSQL oder Postgres Pro** ausgewählt haben:

  - Geben Sie im Feld **PostgreSQL- oder Postgres Pro-Server** den Namen der DBMS-Instanz an. Standardmäßig wird die IP-Adresse des Geräts verwendet, auf dem Kaspersky Security Center installiert wird.

  - Geben Sie im Feld **Port** den Port für die Verbindung des Administrationsservers mit dem DBMS an. Standardmäßig wird Portnummer 5432 verwendet.

  - Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

Schritt 8. Auswählen eines Authentifizierungsmodus

Legen Sie den Authentifizierungsmodus fest, der beim Verbindungsaufbau des Administrationsservers mit dem Datenbankmanagementsystem (DBMS) verwendet werden soll.

In Abhängigkeit vom ausgewählten DBMS können Sie von den folgenden Authentifizierungsmodi auswählen:

- Wählen Sie für SQL Express oder Microsoft SQL Server eine der folgenden Varianten aus:

  - **Microsoft-Windows-Authentifizierungsmodus**. In diesem Fall wird beim Überprüfen der Berechtigungen das Benutzerkonto für den Start des Administrationsservers herangezogen.

  - **SQL Server-Authentifizierungsmodus**. Bei dieser Variante wird für die Überprüfung der Berechtigungen das im Fenster angegebene Benutzerkonto herangezogen. Fülle Sie die Felder **Benutzerkonto** und **Kennwort** aus.

    Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen**.

  Für beide Authentifizierungsmodi untersucht die Anwendung, ob die Datenbank verfügbar ist. Wenn die Datenbank nicht verfügbar ist, wird eine Fehlermeldung angezeigt und Sie müssen die korrekten Anmeldedaten angeben.

  Wenn sich die Administrationsserver-Datenbank auf einem anderen Gerät befindet und das Benutzerkonto des Administrationsservers keinen Zugriff auf den Datenbankserver hat, muss bei der Installation oder dem Update des Administrationsservers die Authentifizierung des SQL-Servers verwendet werden. Dieser Fall kann eintreten, wenn sich das Gerät mit der Datenbank nicht in der Domäne befindet oder der Administrationsserver unter dem Konto "LocalSystem" installiert wurde.

- Geben Sie für MySQL, MariaDB, PostgreSQL oder Postgres Pro das Konto und das Passwort an.

Schritt 9. Auswählen des Benutzerkontos für den Start des Administrationsservers

Wählen Sie ein Benutzerkonto aus, unter dem der Administrationsserver als Dienst gestartet werden soll.

- **Benutzerkonto automatisch erstellen**. Das Programm erstellt ein Benutzerkonto mit dem Namen KL-AK-*, unter dem der Dienst kladminserver ausgeführt wird.

  Sie können diese Variante wählen, wenn Sie planen, den freigegebenen Ordner und das DBMS auf demselben Gerät wie den Administrationsserver unterzubringen.

- **Benutzerkonto auswählen**. Der Dienst des Administrationsservers (kladminserver) wird unter dem ausgewählten Benutzerkonto gestartet.

  Sie müssen ein Domänenbenutzerkonto auswählen, wenn Sie beispielsweise planen, als DBMS eine beliebige Instanz von SQL-Server einschließlich SQL-Express auf einem anderen Gerät zu verwenden, und/oder, wenn Sie planen, den freigegebenen Ordner auf einem anderen Gerät unterzubringen.

  Kaspersky Security Center unterstützt verwaltete Dienstkonten (Managed Service Accounts, MSA) und gruppenverwaltete Dienstkonten (Group Managed Service Accounts, gMSA). Wenn solche Benutzerkonten in Ihrer Domäne verwendet werden, können Sie eines der Konten als Benutzerkonto für den Dienst des Administrationsservers wählen.

Bevor Sie einen MSA oder gMSA angeben, müssen Sie das Konto auf dem gleichen Gerät installieren, auf dem Sie den Administrationsserver installieren möchten. Wenn das Konto noch nicht installiert wurde, beenden Sie die Installation des Administrationsservers, installieren Sie das Konto und starten Sie anschließend die Installation des Administrationsservers erneut. Weitere Informationen zur Installation eines verwalteten Dienstkontos entnehmen Sie bitte der offiziellen Dokumentation von Microsoft.

Um ein MSA oder gMSA anzugeben:

1. Klicken Sie auf die Schaltfläche **Durchsuchen**.
2. Klicken Sie im nächsten Fenster auf die Schaltfläche **Objekttyp**.
3. Wählen Sie den Typ **Benutzerkonto für Dienste** aus und klicken Sie auf **OK**.
4. Wählen Sie das gewünschte Benutzerkonto und klicken Sie auf **OK**.

Das ausgewählte Benutzerkonto muss abhängig davon, welches DBMS Sie verwenden möchten, über verschiedene Rechte verfügen.

Machen Sie aus Gründen der Sicherheit das Benutzerkonto, unter dem der Administrationsserver gestartet wird, nicht privilegiert.

Das Konto des Administrationsservers kann später nicht mehr geändert werden. Wenn Sie ein anderes Administrationsserver-Konto verwenden möchten, müssen das Failover-Cluster neu installieren.

Schritt 10. Auswählen des Benutzerkontos für das Ausführen der Dienste von Kaspersky Security Center

Wählen Sie das Benutzerkonto, unter dem die Dienste von Kaspersky Security Center auf diesem Gerät gestartet werden sollen:

- **Benutzerkonto automatisch erstellen**. Kaspersky Security Center erstellt auf diesem Gerät das lokale Benutzerkonto KlScSvc in der Gruppe kladmins. Die Dienste von Kaspersky Security Center werden unter dem erstellten Benutzerkonto gestartet.
- **Benutzerkonto auswählen**. Die Dienste von Kaspersky Security Center werden unter dem ausgewählten Benutzerkonto gestartet.

  Sie müssen das Domänenbenutzerkonto beispielsweise wählen, wenn Sie planen, Berichte in einem Ordner zu speichern, der sich auf einem anderen Gerät befindet, oder wenn es die Sicherheitsrichtlinie in Ihrer Organisation fordert. Es kann ferner erforderlich sein, bei der Installation des Administrationsservers auf dem Failover-Cluster ein Domänenbenutzerkonto auszuwählen.

Machen Sie aus Gründen der Sicherheit das Benutzerkonto, unter dem die Dienste gestartet werden, nicht privilegiert.

Unter dem ausgewählten Benutzerkonto werden die Dienste des KSN-Proxy-Service (ksnproxy), des Proxy-Service zur Aktivierung von Kaspersky (klactprx) und des Authentifizierungsportals von Kaspersky (klwebsrv) gestartet.

Schritt 11. Festlegen eines gemeinsamen Ordners

Definieren Sie den Speicherort und den Namen des gemeinsamen Ordners, der für folgende Zwecke verwendet wird:

- Die Speicherung der Dateien, die für die Remote-Installation von Programmen benötigt werden (die Dateien werden beim Erstellen der Installationspakete auf den Administrationsserver kopiert).
- Die Speicherung der Updates, die aus den Update-Quellen auf den Administrationsserver kopiert werden.

Allen Benutzern wird für diese Ressource die allgemeine Leseberechtigung erteilt.

Sie können eine der folgenden beiden Varianten auswählen:

- **Freigegebenen Ordner erstellen**: Neuen Ordner erstellen. Geben Sie den Pfad zum Ordner im Feld unten an.
- **Vorhandenen freigegebenen Ordner auswählen**. Gemeinsamen Ordner aus den bereits vorhandenen Ordnern auswählen.

Der Ordner darf sich lokal auf dem Rechner befinden, von dem die Installation erfolgt, oder auf einem Remote-Gerät. Dabei handelt es sich um ein beliebiges Client-Gerät, das zum Netzwerk des Unternehmens gehört. Sie können einen gemeinsamen Ordner durch Klicken auf die Schaltfläche **Durchsuchen** oder manuell angeben, indem Sie den UNC-Pfad in das entsprechende Feld eingeben (Beispiel: \\server\Share).

Standardmäßig wird der lokale Unterordner "KLSHARE" in dem Ordner angelegt, der für die Installation der Programmkomponenten von Kaspersky Security Center angegeben wurde.

Bei Bedarf können Sie den gemeinsamen Ordner später angeben.

Schritt 12. Konfigurieren der Verbindung zum Administrationsserver

Passen Sie die Einstellungen für die Verbindung mit dem Administrationsserver an:

- **Port**

  Nummer des Ports, über den die Verbindung mit dem Administrationsserver erfolgt.

  Standardmäßig wird Portnummer 14000 verwendet.

- **SSL-Port**

  Nummer des SSL-Ports, über den die geschützte Verbindung mit dem Administrationsserver unter Verwendung des SSL-Protokolls erfolgt.

  Standardmäßig wird Portnummer 13000 verwendet.

- **Länge des Chiffrierschlüssels**

  Wählen Sie 1024 Bit oder 2048 Bit als Länge des Chiffrierschlüssels aus.

  Der 1024-Bit-Chiffrierschlüssel reduziert die Auslastung des Prozessors, gilt aber als veraltet und kann in Bezug auf technische Merkmale keine sichere Verschlüsselung gewährleisten. Es besteht zudem die Möglichkeit, dass die vorhandene Hardware mit SSL-Zertifikaten mit einer Schlüssellänge von 1024 Bit nicht kompatibel ist.

Der 2048-Bit-Chiffrierschlüssel erfüllt moderne Verschlüsselungsstandards. Allerdings kann die Verwendung eines 2048-Bit-Chiffrierschlüssels eine zusätzliche Prozessorauslastung zur Folge haben.

Standardmäßig ist **2048 Bit (maximale Sicherheit)** ausgewählt.

Sie können die Einstellungen für die Verbindung mit dem Administrationsserver auch später wie folgt ändern:

- Sie können die Nummern der Ports und SSL-Ports im Administrationsserver im Bereich **Verbindungsports** ändern. Weitere Informationen über die Verbindungsports des Administrationsservers finden Sie im Abschnitt Ports, die von Kaspersky Security Center verwendet werden.
- Wenn Sie das Zertifikat des Administrationsservers mithilfe des Tools "klsetsrvcert" ersetzen, können Sie die Länge des Chiffrierschlüssels mittels des Parameters `-o RsaKeyLen:<Schlüssellänge>` ändern.

Schritt 13. Festlegen der Adresse des Administrationsservers

Geben Sie die Adresse des Administrationsservers auf eine der folgenden Arten an:

- **Name der DNS-Domäne**. Sie können diese Variante verwenden, wenn im Netzwerk ein DNS-Server existiert, den die Client-Geräte verwenden, um die Adresse des Administrationsservers zu beziehen.
- **NetBIOS-Name**. Sie können diese Variante verwenden, wenn die Client-Geräte die Adresse des Administrationsservers mit dem NetBIOS-Protokoll beziehen oder im Netzwerk ein WINS-Server vorhanden ist.
- **IP-Adresse**. Sie können diese Variante verwenden, wenn der Administrationsserver eine statische IP-Adresse aufweist, die sich zu keinem Zeitpunkt ändert.

Wenn Sie Kaspersky Security Center auf dem aktiven Knoten des Kaspersky Security Center Failover-Clusters installieren und Sie bei der Vorbereitung der Cluster-Knoten einen sekundären Netzwerkadapter erstellt haben, geben Sie die IP-Adresse dieses Adapters an. Geben Sie andernfalls die IP-Adresse eines von Ihnen verwendeten Load Balancers eines Drittanbieters ein.

Schritt 14. Adresse des Administrationsservers für die Verbindung mit mobilen Geräten

Dieser Schritt des Installationsassistenten ist verfügbar, wenn Sie die Komponente "Verwaltung mobiler Geräte" für die Installation ausgewählt haben.

Geben Sie im Fenster **Adresse für die Verbindung mobiler Geräte** die externe Adresse des Administrationsservers zur Verbindung mit mobilen Geräten an, die sich außerhalb des lokalen Netzwerks befinden. Sie können die IP-Adresse oder das Domain Name System (DNS) des Administrationsservers angeben.

Schritt 15. Plug-ins für die Programmverwaltung wählen

Wählen Sie die Plug-ins für die Programmverwaltung, die gemeinsam mit Kaspersky Security Center installiert werden sollen.

Für eine erhöhte Benutzerfreundlichkeit bei der Suche sind die Plug-ins je nach Typ der geschützten Objekte in Gruppen unterteilt.

Schritt 16. Entpacken und Installieren der Dateien auf der Festplatte

Nach der Konfiguration der Installationseinstellungen für die Komponenten von Kaspersky Security Center können Sie die Installation auf der Festplatte starten.

Wenn zusätzliche Programme für den Start der Installation erforderlich sind, meldet dies der Installationsassistent vor der Installation von Kaspersky Security Center auf der Seite **Installation der Pflichtkomponenten**. Die erforderlichen Programme werden automatisch nach dem Klicken auf die Schaltfläche **Weiter** installiert.

Auf der letzten Seite können Sie auswählen, welche Konsole für die Arbeit mit Kaspersky Security Center gestartet werden soll:

- **MMC-basierte Verwaltungskonsole starten**
- **Kaspersky Security Center Web Console starten**

  Diese Option ist nur verfügbar, wenn Sie in einem der vorherigen Schritte Kaspersky Security Center Web Console installiert haben.

Sie können außerdem auf **Fertigstellen** klicken, um den Assistenten abzuschließen, ohne Kaspersky Security Center zu verwenden. Sie können später jederzeit mit der Verwendung des Programms beginnen.

Beim ersten Start der Verwaltungskonsole oder Kaspersky Security Center Web Console können Sie eine Erstkonfiguration des Programms ausführen.

Kaspersky Security Center Failover-Cluster bereitstellen

Dieser Abschnitt enthält sowohl allgemeine Informationen zum Kaspersky Security Center Failover-Cluster als auch Anweisungen zur Vorbereitung und Bereitstellung des Kaspersky Security Center Failover-Clusters in Ihrem Netzwerk.

Szenario: Ein Kaspersky Security Center Failover-Cluster bereitstellen

Ein Kaspersky Security Center Failover-Cluster bietet eine hohe Verfügbarkeit für Kaspersky Security Center und minimiert die Ausfallzeit des Administrationsservers im Falle eines Fehlers. Das Failover-Cluster basiert auf zwei identischen Instanzen von Kaspersky Security Center, die auf zwei Computern installiert sind. Eine der Instanzen arbeitet als aktiver Knoten und die andere ist ein passiver Knoten. Der aktive Knoten verwaltet den Schutz der Client-Geräte, während der passive bereit ist, alle Funktionen des aktiven Knotens zu übernehmen, falls der aktive Knoten ausfällt. Wenn ein Fehler auftritt, wird der passive Knoten aktiv und der aktive Knoten wird passiv.

Erforderliche Vorrausetzungen

Sie verfügen über Hardware, welche die Anforderungen für das Failover-Cluster erfüllt.

Schritte

Die Bereitstellung von Kaspersky-Anwendungen erfolgt schrittweise:

1. **Erstellen eines Kontos für die Dienste von Kaspersky Security Center**

   Erstellen Sie eine neue Domänengruppe (in diesem Szenario wird "KLAdmins" für diese Gruppe verwendet) und erteilen Sie der Gruppe anschließend die Berechtigungen des lokalen Administrators auf beiden Knoten und auf dem Dateiserver. Erstellen Sie anschließend zwei neue Domänen-Benutzerkonten (in diesem Szenario werden die Namen "ksc" und "rightless" für diese Konten verwendet) und fügen Sie die Konten der Domänengruppe "KLAdmins" hinzu.

   Fügen Sie das Benutzerkonto, unter dem Kaspersky Security Center installiert wird, zur vorher erstellten Domänengruppe "KLAdmins" hinzu.

2. **Vorbereiten des Dateiservers**

   Bereiten Sie den Dateiserver darauf vor, als Komponente des Kaspersky Security Center Failover-Clusters zu fungieren. Stellen Sie sicher, dass der Dateiserver die Hardware- und Softwareanforderungen erfüllt, erstellen Sie zwei freigegebene Ordner für die Daten von Kaspersky Security Center und konfigurieren Sie die Berechtigungen für den Zugriff auf die freigegebenen Ordner.

   Anleitungen: So bereiten Sie einen Dateiserver für das Kaspersky Security Center Failover-Cluster vor

3. **Vorbereiten von aktiven und passiven Knoten**

   Bereiten Sie zwei Geräte mit identischer Hardware und Software vor, die als aktiver und passiver Knoten fungieren werden.

   Anleitungen: So bereiten Sie Knoten für das Kaspersky Security Center Failover-Cluster vor

4. **Installieren des Datenbankmanagementsystems (DBMS)**

   Wählen Sie eins der unterstützten DBMS aus, und installieren Sie anschließend das DBMS auf einem dedizierten Gerät. Informationen zur Installation eines DBMS finden Sie in dessen Dokumentation.

5. **Installieren von Kaspersky Security Center**

   Installieren Sie Kaspersky Security Center im Modus für Failover-Cluster auf beiden Knoten. Sie müssen Kaspersky Security Center Linux zunächst auf dem Gerät installieren, das Sie als aktiven Host verwenden möchten. Anschließend können Sie es auf dem passiven Host installieren.

   Sie müssen die Kaspersky Security Center Web Console auf einem separaten Gerät installieren, das kein Knoten eines Clusters ist.

   Anleitung: So installieren Sie Kaspersky Security Center auf den Knoten des Kaspersky Security Center Failover-Clusters

6. **Testen des Failover-Clusters**

   Überprüfen Sie, ob Sie das Failover-Cluster richtig konfiguriert haben und ob es ordnungsgemäß funktioniert. Sie können beispielsweise einen der Dienste von Kaspersky Security Center auf dem aktiven Knoten stoppen: kladminserver, klnagent, ksnproxy, klactprx oder klwebsrv. Nach dem Stoppen des Dienstes muss die Verwaltung des Schutzes automatisch auf den passiven Knoten umgeschaltet werden.

Ergebnisse

Das Kaspersky Security Center Failover-Cluster wurde bereitgestellt. Bitte machen Sie sich mit den Ereignissen, die zum Umschalten zwischen aktiven und passiven Knoten führen vertraut.

Über das Kaspersky Security Center Failover-Cluster

Ein Kaspersky Security Center Failover-Cluster bietet eine hohe Verfügbarkeit für Kaspersky Security Center und minimiert die Ausfallzeit des Administrationsservers im Falle eines Fehlers. Das Failover-Cluster basiert auf zwei identischen Instanzen von Kaspersky Security Center, die auf zwei Computern installiert sind. Eine der Instanzen arbeitet als aktiver Knoten und die andere ist ein passiver Knoten. Der aktive Knoten verwaltet den Schutz der Client-Geräte, während der passive bereit ist, alle Funktionen des aktiven Knotens zu übernehmen, falls der aktive Knoten ausfällt. Wenn ein Fehler auftritt, wird der passive Knoten aktiv und der aktive Knoten wird passiv.

Die Verwendung des Failover-Clusters hat keinen Einfluss auf Berechnungen, die auf dem Skalierungshandbuch basieren.

Verwenden Sie zur Fehlerbehebung die Funktion "Kaspersky-Ereignisprotokoll".

Ein geografisch verteiltes Failover-Cluster für Kaspersky Security Center wird nicht unterstützt. Die Bereitstellung eines Failover-Clusters für Kaspersky Security Center ist nur innerhalb eines einzelnen geografischen Standorts möglich.

Umschaltbedingungen

Das Failover-Cluster schaltet die Verwaltung des Schutzes der Client-Geräte vom aktiven Knoten auf den passiven Knoten um, wenn auf dem aktiven Knoten eines der folgenden Ereignisse auftritt:

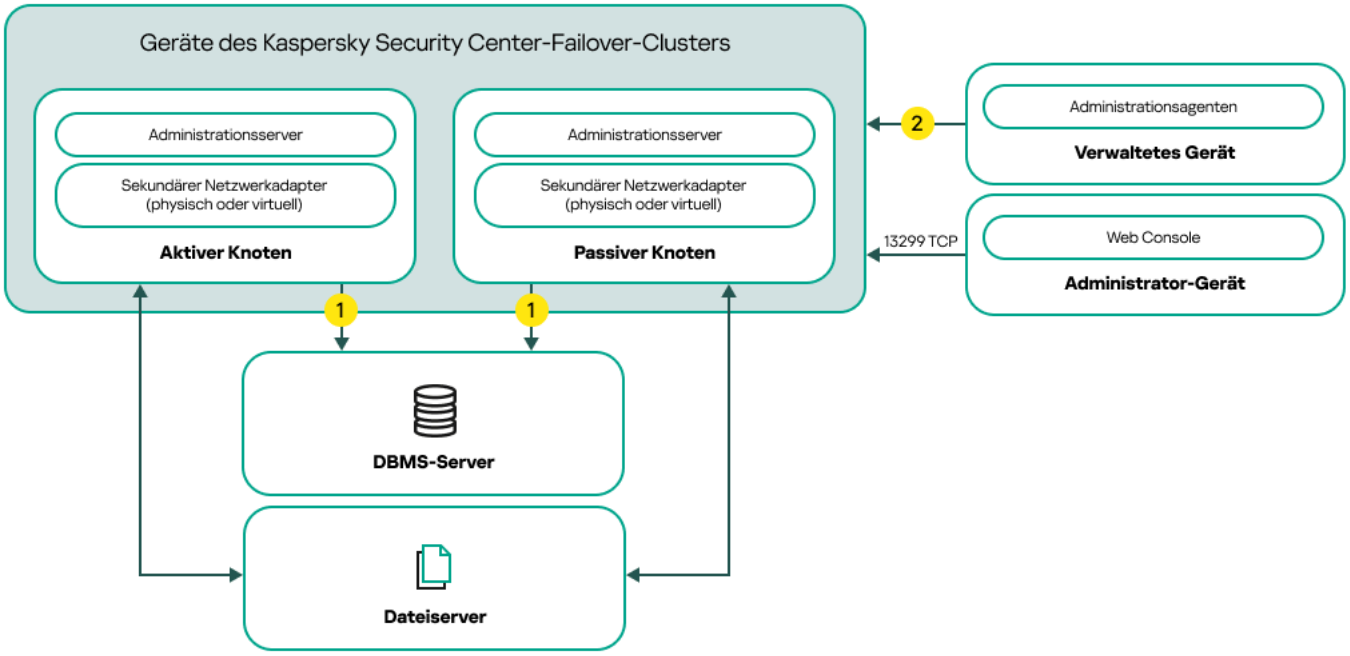
- Der aktive Knoten ist aufgrund eines Software- oder Hardwarefehlers defekt.
- Der aktive Knoten wurde für Wartungsaktivitäten vorübergehend gestoppt.
- Mindestens einer der Dienste (oder Prozesse) von Kaspersky Security Center ist fehlgeschlagen oder wurde vom Benutzer absichtlich beendet. Die Dienste von Kaspersky Security Center sind: kladminserver, klnagent, klactprx und klwebsrv.
- Die Netzwerkverbindung zwischen dem aktiven Knoten und dem Speicher auf dem Dateiserver wurde unterbrochen oder beendet.

Das Failover-Cluster von Kaspersky Security Center verwaltet alle Dienste von Kaspersky Security Center automatisch. Starten Sie die Dienste nicht manuell neu.

Bereitstellungsschemata:

Für die Bereitstellung des Kaspersky Security Center-Failover-Cluster können Sie aus den folgenden Schemata auswählen:

- Schema unter Verwendung eines sekundären Netzwerkadapter.
- Schema unter Verwendung eines Drittanbieter-Load-Balancers.

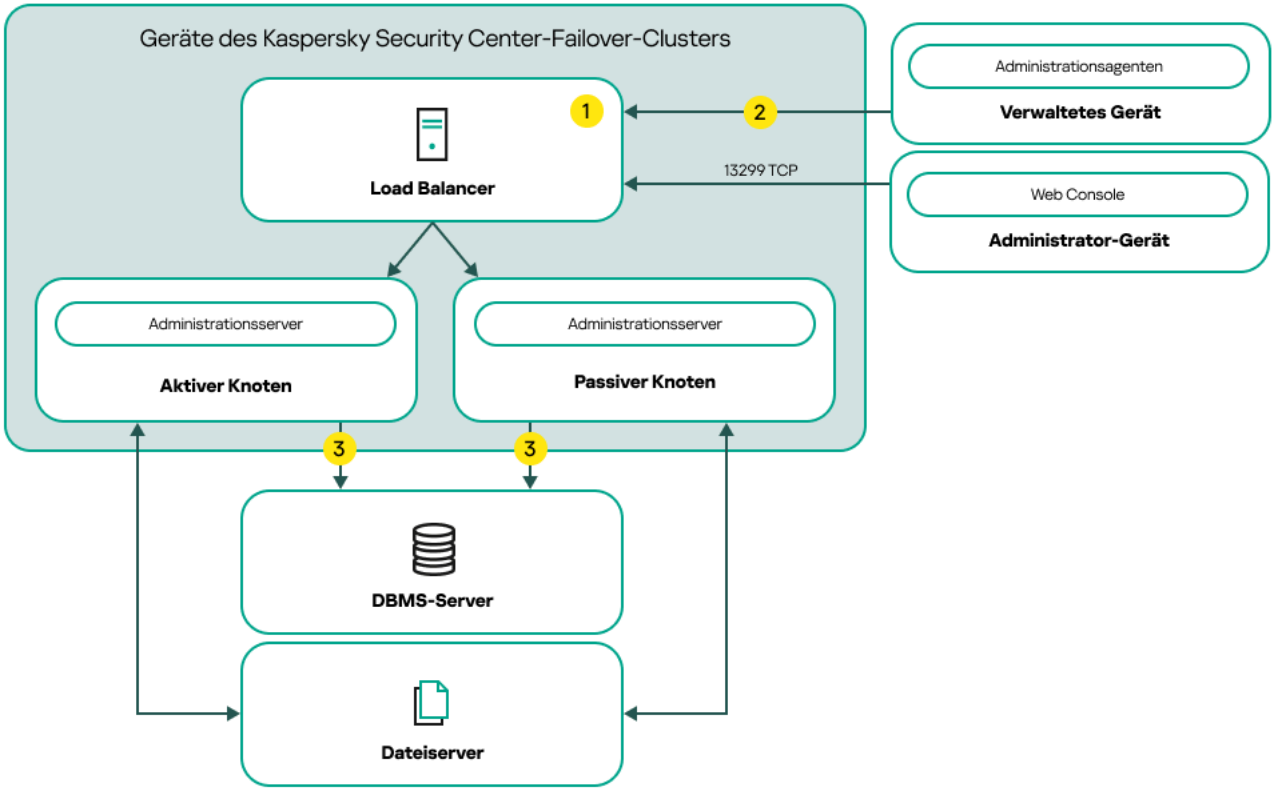


Schema unter Verwendung eines sekundären Netzwerkadapter

Legende des Schemas:

1 Administrationsserver sendet Daten an die Datenbank. Öffnen Sie auf dem Gerät mit der Datenbank die erforderlichen Ports, z. B. Port 3306 für MySQL Server oder Port 1433 für Microsoft SQL Server. Relevante Informationen finden Sie in der DBMS-Dokumentation.

2 Öffnen Sie auf den verwalteten Geräten die folgenden Ports: TCP 13000, UDP 13000 und TCP 17000.



Schema unter Verwendung eines Drittanbieter-Load-Balancers

Legende des Schemas:

1 Öffnen Sie auf dem Gerät des Load-Balancers alle Ports des Administrationsservers: TCP 13000, UDP 13000, TCP 13299 und TCP 17000.

> Wenn Sie das Tool "klakaut" zur Automatisierung verwenden möchten, müssen Sie auch den TCP-Port 13291 öffnen.

2 Öffnen Sie auf den verwalteten Geräten die folgenden Ports: TCP 13000, UDP 13000 und TCP 17000.

3 Administrationsserver sendet Daten an die Datenbank. Öffnen Sie auf dem Gerät mit der Datenbank die erforderlichen Ports, z. B. Port 3306 für MySQL Server oder Port 1433 für Microsoft SQL Server. Relevante Informationen finden Sie in der DBMS-Dokumentation.

Einen Dateiserver für ein Kaspersky Security Center Failover-Cluster vorbereiten

Der Dateiserver ist eine erforderliche Komponente für das Kaspersky Security Center Failover-Cluster.

So bereiten Sie einen Dateiserver vor:

1. Stellen Sie sicher, dass der Dateiserver die Hardware- und Softwareanforderungen erfüllt.
2. Stellen Sie sicher, dass der Dateiserver und beide Knoten (aktiv und passiv) in derselben Domäne enthalten sind oder dass der Dateiserver der Domänencontroller ist.

3. Erstellen Sie zwei freigegebene Ordner auf dem Dateiserver. Einer von ihnen wird verwendet, um Informationen über den Status des Failover-Clusters zu speichern. Der andere dient zum Speichern der Daten und Einstellungen von Kaspersky Security Center. Während der Konfiguration der Installation von Kaspersky Security Center müssen Sie die Pfade zu den freigegebenen Ordnern angeben.

4. Gewähren Sie für die erstellten freigegebenen Ordner volle Zugriffsberechtigungen (sowohl Freigabeberechtigungen als auch NTFS-Berechtigungen) für die folgenden Benutzerkonten und Gruppen:

   - Domänengruppe "KLAdmins".
   - Benutzerkonten $<Knoten_1> und $<Knoten_2>. Dabei entsprechen <Knoten_1> und <Knoten_2> den Gerätenamen der aktiven und passiven Knoten.

Der Dateiserver ist vorbereitet. Um das Kaspersky Security Center Failover-Cluster bereitzustellen, folgen Sie den weiteren Anweisungen in diesem Szenario.

Knoten für ein Kaspersky Security Center Failover-Cluster vorbereiten

Bereiten Sie zwei Geräte darauf vor, um als aktiver und passiver Knoten für ein Kaspersky Security Center Failover-Cluster zu fungieren.

So bereiten Sie die Knoten für ein Kaspersky Security Center Failover-Cluster vor:

1. Stellen Sie sicher, dass Sie über zwei Geräte verfügen, welche die Hardware- und Softwareanforderungen erfüllen. Diese Geräte fungieren als aktive und passive Knoten des Failover-Clusters.

2. Stellen Sie sicher, dass der Dateiserver und beide Knoten in derselben Domäne enthalten sind.

3. Führen Sie eine der folgenden Aktionen aus:

   - Konfigurieren Sie auf jedem der Knoten einen sekundären Netzwerkadapter.

     Ein sekundärer Netzwerkadapter kann physisch oder virtuell sein. Wenn Sie einen physischen Netzwerkadapter verwenden möchten, schließen Sie ihn an und konfigurieren Sie ihn mit den Standardtools des Betriebssystems. Wenn Sie einen virtuellen Netzwerkadapter verwenden möchten, erstellen Sie ihn mithilfe von Drittanbieter-Programmen.

     Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

     - Die sekundären Netzwerkadapter sind deaktiviert.

       Sie können die sekundären Netzwerkadapter im deaktivierten Zustand erstellen oder nach der Erstellung deaktivieren.

     - Die sekundären Netzwerkadapter auf beiden Knoten haben die gleiche IP-Adresse.

   - Verwenden Sie den Load Balancer eines Drittanbieters. Sie können beispielsweise einen nginx-Server verwenden. Gehen Sie in diesem Fall wie folgt vor:

     a. Stellen Sie ein dediziertes Linux-basierten Gerät mit installiertem nginx bereit.

     b. Konfigurieren Sie das Load Balancing. Legen Sie den aktiven Knoten als Hauptserver und den passiven Knoten als Backup-Server fest.

c. Öffnen Sie auf dem nginx-Server alle Ports des Administrationsservers: TCP 13000, UDP 13000, TCP 13299 und TCP 17000.

Wenn Sie das Tool "klakaut" zur Automatisierung verwenden möchten, müssen Sie auch den TCP-Port 13291 öffnen.

4. Starten Sie beide Knoten und den Dateiserver neu.

5. Verknüpfen Sie die beiden freigegebenen Ordner, die Sie während des Schritts zur Vorbereitung des Dateiservers erstellt haben, mit jedem der Knoten. Sie müssen die freigegebenen Ordner als Netzlaufwerke zuordnen. Beim Zuordnen der Ordner können Sie beliebige freie Laufwerksbuchstaben auswählen. Um auf die freigegebenen Ordner zuzugreifen, verwenden Sie die Anmeldeinformationen des Benutzerkontos, das Sie in Schritt 1 des Szenarios erstellt haben.

Die Knoten sind vorbereitet. Um das Kaspersky Security Center Failover-Cluster bereitzustellen, folgen Sie den weiteren Anweisungen des Szenarios.

Kaspersky Security Center auf den Knoten des Kaspersky Security Center Failover-Clusters installieren

Kaspersky Security Center wird auf beiden Knoten des Kaspersky Security Center Failover-Clusters separat installiert. Installieren Sie die Anwendung zunächst auf dem aktiven Knoten und anschließend auf dem passiven. Bei der Installation legen Sie fest, welcher Knoten als aktiv und welcher als passiv fungieren soll.

Nur ein Benutzer aus der Domänengruppe "KLAdmins" kann Kaspersky Security Center auf jedem Knoten installieren.

So installieren Sie Kaspersky Security Center auf dem aktiven Knoten des Kaspersky Security Center Failover-Clusters:

1. Starten Sie die ausführbare Datei "ksc_15.1_<Build Nummer>_full_<Sprache>.exe".

   Es wird ein Fenster geöffnet, in dem Sie die zu installierende Kaspersky-Anwendung auswählen müssen. Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

2. Bitte lesen Sie sorgfältig den Lizenzvertrag und die Datenschutzrichtlinie. Wenn Sie mit allen Punkten des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie im Block **Ich bestätige die vollständige Kenntnis, das Verständnis und das Einverständnis bezüglich** die Kontrollkästchen:

   - **Den Bestimmungen und Bedingungen dieser EULA**
   - **Der Datenschutzrichtlinie, in der die Datenverarbeitung beschrieben wird**

   Die Programminstallation wird nach dem Aktivieren beider Kontrollkästchen fortgesetzt.

   Falls Sie dem Lizenzvertrag oder der Datenschutzrichtlinie nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

3. Wählen Sie **Primärer Knoten des Kaspersky Security Center-Failover-Clusters** aus, um das Programm auf dem aktiven Knoten zu installieren.

4. Gehen Sie im Fenster **Freigegebener Ordner** wie folgt vor:

   - Geben Sie in den Feldern **Status-Netzwerkordner** und **Daten-Netzwerkordner** die Pfade zu den freigegebenen Ordnern an, die Sie auf dem Dateiserver während seiner Einrichtung angelegt haben.
   - Geben Sie in den Feldern **Status-Netzlaufwerk** und **Daten-Netzlaufwerk** die Netzlaufwerke an, mit denen Sie die freigegebenen Ordner während der Einrichtung der Knoten verknüpft haben.
   - Legen Sie den Verbindungsmodus für das Cluster fest: über einen sekundären Netzwerkadapter oder über den Load Balancer eines Drittanbieters.

5. Führen Sie die weitere Schritte einer benutzerdefinierten Installation aus, beginnend mit Schritt 3.

   Geben Sie in Schritt 13 die IP-Adresse eines sekundären Netzwerkadapters an, wenn Sie während der Einrichtung der Cluster-Knoten einen Adapter erstellt haben. Geben Sie andernfalls die IP-Adresse eines von Ihnen verwendeten Load Balancers eines Drittanbieters ein.

Kaspersky Security Center wird auf dem aktiven Knoten installiert.

So installieren Sie Kaspersky Security Center auf dem passiven Knoten des Kaspersky Security Center Failover-Clusters:

1. Starten Sie die ausführbare Datei "ksc_15.1_<Build Nummer>_full_<Sprache>.exe".

   Es wird ein Fenster geöffnet, in dem Sie die zu installierende Kaspersky-Anwendung auswählen müssen. Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

2. Bitte lesen Sie sorgfältig den Lizenzvertrag und die Datenschutzrichtlinie. Wenn Sie mit allen Punkten des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie im Block **Ich bestätige die vollständige Kenntnis, das Verständnis und das Einverständnis bezüglich** die Kontrollkästchen:

   - **Den Bestimmungen und Bedingungen dieser EULA**
   - **Der Datenschutzrichtlinie, in der die Datenverarbeitung beschrieben wird**

   Die Programminstallation wird nach dem Aktivieren beider Kontrollkästchen fortgesetzt.

   Falls Sie dem Lizenzvertrag oder der Datenschutzrichtlinie nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

3. Wählen Sie **Sekundärer Knoten des Kaspersky Security Center-Failover-Clusters** aus, um das Programm auf dem passiven Knoten zu installieren.

4. Geben Sie im Feld **Status-Netzwerkordner** des Fensters **Freigegebener Ordner** den Pfad zu dem Ordner mit den Informationen über das Cluster-State an, den Sie auf dem Dateiserver während seiner Einrichtung angegeben haben.

5. Klicken Sie auf die Schaltfläche **Installieren**. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche **Fertigstellen**.

Kaspersky Security Center wird auf dem passiven Knoten installiert. Sie können jetzt das Kaspersky Security Center Failover-Cluster testen, um sicherzustellen, dass Sie es richtig konfiguriert haben und dass das Cluster ordnungsgemäß funktioniert.

Cluster-Knoten manuell starten und beenden

Möglicherweise müssen Sie das gesamten Kaspersky Security Center Failover-Cluster stoppen oder einen der Cluster-Knoten zu Wartungszwecken vorübergehend trennen. Folgen Sie in diesem Fall den Anweisungen in diesem Abschnitt. Versuchen Sie nicht, die Dienste oder Prozesse im Zusammenhang mit dem Failover-Cluster auf eine andere Weise zu starten oder zu stoppen. Dies kann zu Datenverlust führen.

Starten und Stoppen des gesamten Failover-Clusters zu Wartungszwecken

So starten oder stoppen Sie das gesamten Failover-Cluster:

1. Wechseln Sie auf dem aktiven Knoten zu <Laufwerk>:\Programme (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Öffnen Sie die Befehlszeile und führen Sie einen der folgenden Befehle aus:
   - Um das Cluster zu stoppen: `klfoc -stopcluster --stp klfoc`
   - Um das Cluster zu starten: `klfoc -startcluster --stp klfoc`

Das Failover-Cluster wird je nach ausgeführtem Befehl gestartet oder gestoppt.

Wartung eines Knotens

So warten Sie einen der Knoten:

1. Stoppen Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -stopcluster --stp klfoc`.
2. Wechseln Sie auf dem Knoten, den Sie warten möchten, zu <Laufwerk>:\Programme (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Öffnen Sie die Befehlszeile, und trennen Sie anschließend den Knoten vom Cluster, indem Sie den Befehl `detach_node.cmd` ausführen.
4. Starten Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -startcluster --stp klfoc`.
5. Führen Sie die Wartungsarbeiten durch.
6. Stoppen Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -stopcluster --stp klfoc`.
7. Wechseln Sie auf dem verwalteten Knoten zu <Laufwerk>:\Programme (x86)\Kaspersky Lab\Kaspersky Security Center.

8. Öffnen Sie die Befehlszeile, und fügen Sie den Knoten anschließend wieder an das Cluster an, indem Sie die Befehl `attach_node.cmd` ausführen.

9. Starten Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -startcluster --stp klfoc`.

Der Knoten ist gewartet und an das Failover-Cluster angehängt.

Installation des Administrationsservers in einem Windows Server Failover-Cluster

Das Verfahren zur Installation eines Administrationsservers auf einem Failovercluster unterscheidet sich sowohl von der Standardinstallation als auch von der benutzerdefinierten Installation auf einem eigenständigen Gerät.

> Geografisch verteilte Windows-basierte Failover-Cluster werden nicht unterstützt. Die Bereitstellung eines Failover-Clusters auf Basis von Windows Server ist nur innerhalb eines einzelnen geografischen Standorts möglich, der eine hohe Netzwerkverfügbarkeit und eine schnelle Reaktionszeit zwischen den Cluster-Knoten bietet.

Führen Sie die in diesem Abschnitt beschriebenen Schritte auf dem Knoten aus, der einen gemeinsamen Datenspeicher des Clusters enthält.

Um Kaspersky Security Center Administrationsserver auf einem Cluster zu installieren:

Starten Sie die ausführbare Datei "ksc_<Versionsnummer>.<Buildnummer>_full_<Sprache der Lokalisierung>.exe".

Ein Fenster wird geöffnet, in dem Sie Kaspersky-Anwendungen zur Installation auswählen können. Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

Schritt 1. Anzeigen des Lizenzvertrags und der Datenschutzrichtlinie

Machen Sie sich in diesem Schritt des Installationsassistenten mit dem Lizenzvertrag vertraut, den Sie mit Kaspersky abschließen, sowie mit der Datenschutzrichtlinie.

Außerdem werden Sie eventuell aufgefordert, sich mit den Lizenzverträgen und Datenschutzrichtlinien für die im Programmpaket von Kaspersky Security Center verfügbaren Plug-ins für die Programmverwaltung vertraut zu machen.

Bitte lesen Sie sorgfältig den Lizenzvertrag und die Datenschutzrichtlinie. Wenn Sie mit allen Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, bestätigen Sie dies durch das Aktivieren der entsprechenden Kontrollkästchen.

Die Programminstallation wird nach dem Aktivieren beider Kontrollkästchen fortgesetzt.

Falls Sie dem Lizenzvertrag oder der Datenschutzrichtlinie nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

Schritt 2. Auswählen des Installationstyps in dem Cluster

Wählen Sie den Installationstyp in dem Cluster aus:

- **Cluster (auf allen Clusterknoten installieren)**

  Dies ist die empfohlene Option. Wenn Sie diese Option auswählen, wird der Administrationsserver gleichzeitig auf allen Knoten des Clusters installiert.

  > Im Schritt Auswählen der Verwaltungskonsole für die Installation, müssen Sie die Konsole auswählen, die auf dem aktuellen Cluster-Knoten installiert wird. Wenn Sie eine Konsole ausschließlich auf diesem Cluster-Knoten installieren, verlieren Sie im Falle eines Knotenausfalls den Zugriff auf den Administrationsserver. Wir empfehlen, dass Sie in diesem Schritt, die MMC-basierte Verwaltungskonsole zur Installation auf allen Cluster-Knoten auswählen. Nachdem Sie den Administrationsserver installiert haben, sollten Sie die Kaspersky Security Center Web Console auf einem separaten Gerät installieren, das selbst kein Knoten eines Clusters ist. Auf diese Weise können Sie den Administrationsserver mithilfe der Kaspersky Security Center Web Console weiterhin verwalten, wenn der Cluster-Knoten ausfällt.

- **Lokal (nur auf diesem Gerät installieren)**

  Wenn Sie diese Option auswählen, wird der Administrationsserver nur auf dem aktuellen Knoten installiert, so als wäre er auf einem eigenständigen Server. Der Administrationsserver funktioniert dann nicht als cluster-fähige Anwendung. Beispielsweise können Sie diese Option auswählen, um gemeinsam genutzten Speicherplatz zu sparen, wenn für den Administrationsserver keine Fehlertoleranz erforderlich ist. Im Falle eines Fehlers auf dem aktuellen Knoten müssen Sie den Administrationsserver auf einem anderen Knoten installieren und den Zustand des Administrationsservers aus einem Backup wiederherstellen.

Die weitere Schritte sind dieselben wie bei Verwendung der standardmäßigen oder benutzerdefinierten Installationsmethode, beginnend mit Schritt zur Auswahl der Installationsmethode.

Schritt 3. Angeben des Namens des virtuellen Administrationsservers

Geben Sie den Netzwerknamen des neuen virtuellen Administrationsservers an. Mit diesem Namen können Sie die Verwaltungskonsole oder die Kaspersky Security Center Web Console mit dem Administrationsserver verbinden.

Der von Ihnen angegebene Name muss vom Clusternamen abweichen.

Schritt 4. Angeben der Netzwerkdetails des virtuellen Administrationsservers

Um die Informationen zum Netzwerk der neuen Instanz des virtuellen Administrationsservers anzugeben:

1. Wählen Sie unter **Zu verwendendes Netzwerk** das Domänennetzwerk aus, mit dem der aktuelle Clusterknoten verbunden ist.
2. Führen Sie eine beliebige der folgenden Aktionen aus:
   - Wenn im ausgewählten Netzwerk DHCP zum Zuweisen von IP-Adressen verwendet wird, aktivieren Sie die Option **DHCP verwenden**.
   - Wenn im ausgewählten Netzwerk kein DHCP verwendet wird, geben Sie die erforderliche IP-Adresse an.

     Die von Ihnen angegebene IP-Adresse muss von der Cluster-IP-Adresse abweichen.
3. Klicken Sie auf **Hinzufügen**, um die angegebenen Einstellungen zu übernehmen.

Sie können die automatisch zugewiesene oder die angegebene IP-Adresse verwenden, um die Verwaltungskonsole oder die Kaspersky Security Center Web Console mit dem Administrationsserver zu verbinden.

Schritt 5. Angeben einer Clustergruppe

Eine Clustergruppe ist eine spezielle Rolle eines Failover-Clusters, die gemeinsame Ressourcen für alle Knoten enthält. Sie haben zwei Optionen:

- Erstellen einer neuen Clustergruppe.

  Diese Option wird in den meisten Fällen empfohlen. Die neue Clustergruppe enthält alle gemeinsamen Ressourcen, die sich auf die Instanz des Administrationsservers beziehen.

- Auswählen einer vorhandenen Clustergruppe.

  Wählen Sie diese Option aus, wenn Sie eine gemeinsame Ressource verwenden möchten, die bereits einer vorhandenen Clustergruppe zugeordnet ist. Beispielsweise können Sie diese Option verwenden, wenn Sie einen Speicher verwenden möchten, der einer vorhandenen Clustergruppe zugeordnet ist, und wenn für eine neue Clustergruppe kein anderer Speicher verfügbar ist.

Schritt 6. Auswählen eines Cluster-Datenspeichers

Um den Datenspeicher eines Clusters auszuwählen:

1. **Wählen Sie unter Verfügbaren Datenverwaltungen** den Datenspeicher aus, auf dem die gemeinsamen Ressourcen der Instanz des virtuellen Administrationsservers installiert werden sollen.
2. Wenn der ausgewählte Datenspeicher mehrere Volumes enthält, wählen Sie unter **Verfügbare Bereiche auf dem Laufwerk** das gewünschte Volume aus.
3. Geben Sie unter **Installationspfad** den Pfad im gemeinsamen Datenspeicher ein, in dem die Ressourcen der Instanz des virtuellen Administrationsservers installiert werden sollen.

Der Datenspeicher ist ausgewählt.

Schritt 7. Angeben eines Kontos für die Remote-Installation

Geben Sie den Benutzernamen und das Kennwort an, die für die Remote-Installation der Instanz des virtuellen Administrationsservers auf einem passiven Knoten des Clusters verwendet werden sollen.

Das von Ihnen angegebene Konto muss auf allen Knoten des Clusters über Administratorberechtigungen verfügen.

Schritt 8. Auswählen der zu installierenden Komponenten

Wählen Sie die Komponenten des Kaspersky Security Center Administrationsservers aus, die installiert werden sollen:

- **Verwaltung mobiler Geräte**. Aktivieren Sie dieses Kontrollkästchen, wenn während der Ausführung des Installationsassistenten von Kaspersky Security Center Installationspakete für mobile Geräte erstellt werden sollen. Sie können die Installationspakete für mobile Geräte nach der Installation des Administrationsservers auch manuell über die Verwaltungskonsole erstellen.
- **SNMP-Agent**. Empfängt statistische Daten für den Administrationsserver mit dem SNMP-Protokoll. Die Komponente steht zur Verfügung, wenn bei der Installation des Programms auf dem Gerät die SNMP-Komponente installiert ist.

  Nach der Installation von Kaspersky Security Center befinden sich die für den Empfang von Statistikdaten benötigten mib-Dateien im Installationsverzeichnis im Unterordner SNMP.

Die Komponenten Administrationsagent und Verwaltungskonsole werden in der Liste der Komponenten nicht angezeigt. Diese Komponenten werden automatisch installiert und deren Installation kann nicht abgebrochen werden.

Geben Sie in diesem Schritt des Assistenten auch den Ordner für die Installation der Komponenten des Administrationsservers an. Standardmäßig werden die Komponenten in den Ordner <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center installiert. Wenn kein Ordner mit diesem Namen vorhanden ist, wird er automatisch während des Installationsvorgangs angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** ändern.

Schritt 9. Auswählen der Netzwerkgröße

Geben Sie die Größe des Netzwerks an, in dem Kaspersky Security Center installiert werden soll. Der Assistent berücksichtigt die Anzahl der Geräte im Netzwerk und passt die Installationseinstellungen und die Darstellung der Programmoberfläche dementsprechend an.

In der Tabelle unten sind die Installationseinstellungen für das Programm und die Darstellung der Programmoberfläche bei Auswahl von verschiedenen Netzwerkgrößen aufgeführt.

Installationseinstellungen je nach Netzwerkgröße

Einstellungen	1 – 100 verwaltete Geräte	101 – 1.000 verwaltete Geräte	1.001 – 5.000 verwaltete Geräte	Mehr als 5.000 verwaltete Geräte
Mit dem Knoten des sekundären und virtuellen Administrationsservers, sowie mit allen Einstellungen, die für sekundäre und virtuelle Administrationsserver relevant sind, in der Konsolenstruktur anzeigen (nur in der MMC-basierten Verwaltungskonsole verfügbar)	Nicht vorhanden	Nicht vorhanden	Vorhanden	Vorhanden
Mit den Abschnitten **Sicherheit** in den Eigenschaftsfenstern des Administrationsservers und der Administrationsgruppen anzeigen (nur in der MMC-basierten Verwaltungskonsole verfügbar)	Nicht vorhanden	Nicht vorhanden	Vorhanden	Vorhanden
Zufällige Verteilung der Startzeit für die Update-Aufgabe auf Client-Geräten	Nicht vorhanden	im Abstand von 5 Minuten	im Abstand von 10 Minuten	im Abstand von 10 Minuten

Falls Sie den Administrationsserver mit einem MySQL 5.7, oder SQL Express-Datenbankserver verbinden, wird es nicht empfohlen, das Programm zur Verwaltung von mehr als 10.000 Geräten zu verwenden. Für das MariaDB-DBMS beträgt die empfohlene maximale Anzahl verwalteter Geräte 20.000 Stück.

Schritt 10. Auswählen der Datenbank

Wählen Sie in diesem Schritt des Assistenten eins der folgenden Datenbankverwaltungssysteme (DBMS) aus, welches zum Speichern der Administrationsserver-Datenbank verwendet wird:

- **Microsoft SQL Server oder SQL Server Express**
- **MySQL oder MariaDB**
- **PostgreSQL oder Postgres Pro**

Es wird empfohlen, den Administrationsserver anstatt auf einem Domänencontroller auf einem dezidierten Server zu installieren. Wenn Sie Kaspersky Security Center jedoch auf einem Server installieren, der als schreibgeschützter Domänencontroller (RODC) agiert, muss Microsoft SQL Server (SQL Express) nicht lokal (auf demselben Gerät) installiert werden. In diesem Fall empfehlen wir Ihnen, Microsoft SQL Server (SQL Express) per Fernzugriff (auf einem anderen Gerät) zu installieren, oder MySQL, MariaDB oder PostgreSQL zu verwenden, falls Sie das DBMS lokal installieren müssen.

Die Datenbankstruktur des Administrationsservers ist in der Datei klakdb.chm enthalten, die sich im Installationsordner von Kaspersky Security Center befindet. Diese Datei ist auch als Archiv auf dem Kaspersky-Portal verfügbar: klakdb.zip.

Schritt 11. Konfigurieren des SQL-Servers

Geben Sie in diesem Schritt des Assistenten je nach ausgewähltem Datenbankverwaltungssystem (DBMS) die folgenden Verbindungseinstellungen an:

- Wenn Sie im vorherigen Schritt **Microsoft SQL Server oder SQL Server Express** ausgewählt haben:

  - Geben Sie im Feld **Name der SQL Server-Instanz** den Namen des SQL-Servers an, der im Netzwerk installiert ist. Mit der Schaltfläche **Durchsuchen** kann die Liste aller im Netzwerk installierten SQL-Server angezeigt werden. Standardmäßig ist dieses Feld leer.

    Wenn Sie eine Verbindung über einen benutzerdefinierten Port zum SQL Server herstellen, geben Sie den Hostnamen des SQL Servers zusammen mit der durch ein Komma getrennten Portnummer an, z. B.:

    ```
    SQL_Server_host_name,1433
    ```

    Wenn Sie die Kommunikation zwischen dem Administrationsserver und SQL Server mittels eines Zertifikats absichern, geben Sie im Feld **Name der SQL Server-Instanz** denselben Hostnamen an, der beim Generieren des Zertifikats verwendet wurde. Wenn Sie eine benannte Instanz von SQL Server verwenden, geben Sie den Hostnamen des SQL-Servers zusammen mit der durch ein Komma getrennten Portnummer an, z. B.:

    ```
    SQL_Server_name,1433
    ```

    Wenn Sie mehrere Instanzen von SQL-Servern auf demselben Host verwenden, geben Sie zusätzlich den durch einen Backslash getrennten Instanznamen an, z. B.:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Wenn auf einem SQL Server im Unternehmensnetzwerk die Always-On-Funktion aktiviert ist, geben Sie den Namen des Verfügbarkeitsgruppenlisteners im Feld **Name der SQL Server-Instanz** an. Beachten Sie, dass der Administrationsserver den Verfügbarkeitsmodus für synchrone Commits nur unterstützt, wenn die Always-On-Funktion aktiviert ist.

  - Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

  Wenn Sie auf diesem Schritt einen SQL-Server manuell auf demselben Gerät installieren möchten, von dem aus die Installation von Kaspersky Security Center erfolgt, müssen Sie die Installation abbrechen und sie nach der Installation des SQL-Servers erneut starten. Die unterstützten SQL-Server werden in den Systemanforderungen aufgezählt.

  Wenn Sie einen SQL-Server auf einem Remote-Gerät installieren wollen, muss der Installationsassistent für Kaspersky Security Center nicht abgebrochen werden. Installieren Sie den SQL-Server, und fahren Sie mit der Installation von Kaspersky Security Center fort.

- Wenn Sie im vorherigen Schritt **MySQL oder MariaDB** ausgewählt haben:

  - Geben Sie im Feld **Name der SQL Server-Instanz** den Namen der DBMS-Instanz an. Standardmäßig wird die IP-Adresse des Geräts verwendet, auf dem Kaspersky Security Center installiert wird.

  - Geben Sie im Feld **Port** den Port für die Verbindung des Administrationsservers mit dem DBMS an. Standardmäßig wird Portnummer 3306 verwendet.

  - Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

- Wenn Sie im vorherigen Schritt **PostgreSQL oder Postgres Pro** ausgewählt haben:

  - Geben Sie im Feld **PostgreSQL- oder Postgres Pro-Server** den Namen der DBMS-Instanz an. Standardmäßig wird die IP-Adresse des Geräts verwendet, auf dem Kaspersky Security Center installiert wird.

  - Geben Sie im Feld **Port** den Port für die Verbindung des Administrationsservers mit dem DBMS an. Standardmäßig wird Portnummer 5432 verwendet.

Geben Sie im Feld **Name der Datenbank** den Namen des DBMS ein, das zum Speichern der Daten des Administrationsservers erstellt wurde. Standardmäßig ist der Wert auf *KAV* eingestellt.

Schritt 12. Auswählen eines Authentifizierungsmodus

Legen Sie den Authentifizierungsmodus fest, der beim Verbindungsaufbau des Administrationsservers mit dem Datenbankmanagementsystem (DBMS) verwendet werden soll.

In Abhängigkeit vom ausgewählten DBMS können Sie von den folgenden Authentifizierungsmodi auswählen:

- Wählen Sie für SQL Express oder Microsoft SQL Server eine der folgenden Varianten aus:

  - **Microsoft-Windows-Authentifizierungsmodus**. In diesem Fall wird beim Überprüfen der Berechtigungen das Benutzerkonto für den Start des Administrationsservers herangezogen.

  - **SQL Server-Authentifizierungsmodus**. Bei dieser Variante wird für die Überprüfung der Berechtigungen das im Fenster angegebene Benutzerkonto herangezogen. Fülle Sie die Felder **Benutzerkonto** und **Kennwort** aus.

    Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen**.

  Für beide Authentifizierungsmodi untersucht die Anwendung, ob die Datenbank verfügbar ist. Wenn die Datenbank nicht verfügbar ist, wird eine Fehlermeldung angezeigt und Sie müssen die korrekten Anmeldedaten angeben.

  Wenn sich die Administrationsserver-Datenbank auf einem anderen Gerät befindet und das Benutzerkonto des Administrationsservers keinen Zugriff auf den Datenbankserver hat, muss bei der Installation oder dem Update des Administrationsservers die Authentifizierung des SQL-Servers verwendet werden. Dieser Fall kann eintreten, wenn sich das Gerät mit der Datenbank nicht in der Domäne befindet oder der Administrationsserver unter dem Konto "LocalSystem" installiert wurde.

Geben Sie für MySQL, MariaDB, PostgreSQL oder Postgres Pro das Konto und das Passwort an.

Schritt 13. Auswählen des Benutzerkontos für den Start des Administrationsservers

Wählen Sie ein Benutzerkonto aus, unter dem der Administrationsserver als Dienst gestartet werden soll.

- **Benutzerkonto automatisch erstellen**. Das Programm erstellt ein Benutzerkonto mit dem Namen KL-AK-*, unter dem der Dienst kladminserver ausgeführt wird.

  Sie können diese Variante wählen, wenn Sie planen, den freigegebenen Ordner und das DBMS auf demselben Gerät wie den Administrationsserver unterzubringen.

- **Benutzerkonto auswählen**. Der Dienst des Administrationsservers (kladminserver) wird unter dem ausgewählten Benutzerkonto gestartet.

  Sie müssen ein Domänenbenutzerkonto auswählen, wenn Sie beispielsweise planen, als DBMS eine beliebige Instanz von SQL-Server einschließlich SQL-Express auf einem anderen Gerät zu verwenden, und/oder, wenn Sie planen, den freigegebenen Ordner auf einem anderen Gerät unterzubringen.

  Kaspersky Security Center unterstützt verwaltete Dienstkonten (Managed Service Accounts, MSA) und gruppenverwaltete Dienstkonten (Group Managed Service Accounts, gMSA). Wenn solche Benutzerkonten in Ihrer Domäne verwendet werden, können Sie eines der Konten als Benutzerkonto für den Dienst des Administrationsservers wählen.

  Bevor Sie einen MSA oder gMSA angeben, müssen Sie das Konto auf dem gleichen Gerät installieren, auf dem Sie den Administrationsserver installieren möchten. Wenn das Konto noch nicht installiert wurde, beenden Sie die Installation des Administrationsservers, installieren Sie das Konto und starten Sie anschließend die Installation des Administrationsservers erneut. Weitere Informationen zur Installation eines verwalteten Dienstkontos entnehmen Sie bitte der offiziellen Dokumentation von Microsoft.

  Um ein MSA oder gMSA anzugeben:

  1. Klicken Sie auf die Schaltfläche **Durchsuchen**.
  2. Klicken Sie im nächsten Fenster auf die Schaltfläche **Objekttyp**.
  3. Wählen Sie den Typ **Benutzerkonto für Dienste** aus und klicken Sie auf **OK**.
  4. Wählen Sie das gewünschte Benutzerkonto und klicken Sie auf **OK**.

Das ausgewählte Benutzerkonto muss abhängig davon, welches DBMS Sie verwenden möchten, über verschiedene Rechte verfügen.

Machen Sie aus Gründen der Sicherheit das Benutzerkonto, unter dem der Administrationsserver gestartet wird, nicht privilegiert.

Das Konto des Administrationsservers kann später nicht mehr geändert werden. Wenn Sie ein anderes Administrationsserver-Konto verwenden möchten, müssen das Failover-Cluster neu installieren.

Schritt 14. Auswählen des Benutzerkontos für das Ausführen der Dienste von Kaspersky Security Center

Wählen Sie das Benutzerkonto, unter dem die Dienste von Kaspersky Security Center auf diesem Gerät gestartet werden sollen:

- **Benutzerkonto automatisch erstellen**. Kaspersky Security Center erstellt auf diesem Gerät das lokale Benutzerkonto KlScSvc in der Gruppe kladmins. Die Dienste von Kaspersky Security Center werden unter dem erstellten Benutzerkonto gestartet.

- **Benutzerkonto auswählen**. Die Dienste von Kaspersky Security Center werden unter dem ausgewählten Benutzerkonto gestartet.

  Sie müssen das Domänenbenutzerkonto beispielsweise wählen, wenn Sie planen, Berichte in einem Ordner zu speichern, der sich auf einem anderen Gerät befindet, oder wenn es die Sicherheitsrichtlinie in Ihrer Organisation fordert. Es kann ferner erforderlich sein, bei der Installation des Administrationsservers auf dem Failover-Cluster ein Domänenbenutzerkonto auszuwählen.

Machen Sie aus Gründen der Sicherheit das Benutzerkonto, unter dem die Dienste gestartet werden, nicht privilegiert.

Unter dem ausgewählten Benutzerkonto werden die Dienste des KSN Proxy-Service (ksnproxy), des Proxy-Service zur Aktivierung von Kaspersky (klactprx) und des Authentifizierungsportals von Kaspersky (klwebsrv) gestartet.

Schritt 15. Festlegen eines gemeinsamen Ordners

Definieren Sie den Speicherort und den Namen des gemeinsamen Ordners, der für folgende Zwecke verwendet wird:

- Die Speicherung der Dateien, die für die Remote-Installation von Programmen benötigt werden (die Dateien werden beim Erstellen der Installationspakete auf den Administrationsserver kopiert).

- Die Speicherung der Updates, die aus den Update-Quellen auf den Administrationsserver kopiert werden.

Allen Benutzern wird für diese Ressource die allgemeine Leseberechtigung erteilt.

Sie können eine der folgenden beiden Varianten auswählen:

- **Freigegebenen Ordner erstellen**: Neuen Ordner erstellen. Geben Sie den Pfad zum Ordner im Feld unten an.

- **Vorhandenen freigegebenen Ordner auswählen**. Gemeinsamen Ordner aus den bereits vorhandenen Ordnern auswählen.

Der Ordner darf sich lokal auf dem Rechner befinden, von dem die Installation erfolgt, oder auf einem Remote-Gerät. Dabei handelt es sich um ein beliebiges Client-Gerät, das zum Netzwerk des Unternehmens gehört. Sie können einen gemeinsamen Ordner durch Klicken auf die Schaltfläche **Durchsuchen** oder manuell angeben, indem Sie den UNC-Pfad in das entsprechende Feld eingeben (Beispiel: \\server\Share).

Standardmäßig wird der lokale Unterordner "KLSHARE" in dem Ordner angelegt, der für die Installation der Programmkomponenten von Kaspersky Security Center angegeben wurde.

Bei Bedarf können Sie den gemeinsamen Ordner später angeben.

Schritt 16. Konfigurieren der Verbindung zum Administrationsserver

Passen Sie die Einstellungen für die Verbindung mit dem Administrationsserver an:

- **Port**

  Nummer des Ports, über den die Verbindung mit dem Administrationsserver erfolgt.

  Standardmäßig wird Portnummer 14000 verwendet.

- **SSL-Port**

  Nummer des SSL-Ports, über den die geschützte Verbindung mit dem Administrationsserver unter Verwendung des SSL-Protokolls erfolgt.

  Standardmäßig wird Portnummer 13000 verwendet.

- **Länge des Chiffrierschlüssels**

  Wählen Sie 1024 Bit oder 2048 Bit als Länge des Chiffrierschlüssels aus.

  Der 1024-Bit-Chiffrierschlüssel reduziert die Auslastung des Prozessors, gilt aber als veraltet und kann in Bezug auf technische Merkmale keine sichere Verschlüsselung gewährleisten. Es besteht zudem die Möglichkeit, dass die vorhandene Hardware mit SSL-Zertifikaten mit einer Schlüssellänge von 1024 Bit nicht kompatibel ist.

  Der 2048-Bit-Chiffrierschlüssel erfüllt moderne Verschlüsselungsstandards. Allerdings kann die Verwendung eines 2048-Bit-Chiffrierschlüssels eine zusätzliche Prozessorauslastung zur Folge haben.

  Standardmäßig ist **2048 Bit (maximale Sicherheit)** ausgewählt.

Sie können die Einstellungen für die Verbindung mit dem Administrationsserver auch später wie folgt ändern:

- Sie können die Nummern der Ports und SSL-Ports im Administrationsserver im Bereich **Verbindungsports** ändern. Weitere Informationen über die Verbindungsports des Administrationsservers finden Sie im Abschnitt Ports, die von Kaspersky Security Center verwendet werden.

- Wenn Sie das Zertifikat des Administrationsservers mithilfe des Tools "klsetsrvcert" ersetzen, können Sie die Länge des Chiffrierschlüssels mittels des Parameters `-o RsaKeyLen:<Schlüssellänge>` ändern.

Schritt 17. Festlegen der Adresse des Administrationsservers

Legen Sie die Adresse des Administrationsservers fest. Sie können eine der folgenden Varianten auswählen:

- **Name der DNS-Domäne**. Sie können diese Variante verwenden, wenn im Netzwerk ein DNS-Server existiert, den die Client-Geräte verwenden, um die Adresse des Administrationsservers zu beziehen.

- **NetBIOS-Name**. Sie können diese Variante verwenden, wenn die Client-Geräte die Adresse des Administrationsservers mit dem NetBIOS-Protokoll beziehen oder im Netzwerk ein WINS-Server vorhanden ist.

- **IP-Adresse**. Sie können diese Variante verwenden, wenn der Administrationsserver eine statische IP-Adresse aufweist, die sich zu keinem Zeitpunkt ändert.

Schritt 18. Adresse des Administrationsservers für die Verbindung mit mobilen Geräten

Dieser Schritt des Installationsassistenten ist verfügbar, wenn Sie die Komponente "Verwaltung mobiler Geräte" für die Installation ausgewählt haben.

Geben Sie im Fenster **Adresse für die Verbindung mobiler Geräte** die externe Adresse des Administrationsservers zur Verbindung mit mobilen Geräten an, die sich außerhalb des lokalen Netzwerks befinden. Sie können die IP-Adresse oder das Domain Name System (DNS) des Administrationsservers angeben.

Schritt 19. Entpacken und Installieren der Dateien auf der Festplatte

Nach der Konfiguration der Installationseinstellungen für die Komponenten von Kaspersky Security Center können Sie die Installation auf der Festplatte starten.

Wenn zusätzliche Programme für den Start der Installation erforderlich sind, meldet dies der Installationsassistent vor der Installation von Kaspersky Security Center auf der Seite **Installation der Pflichtkomponenten**. Die erforderlichen Programme werden automatisch nach dem Klicken auf die Schaltfläche **Weiter** installiert.

Auf der letzten Seite können Sie auswählen, welche Konsole für die Arbeit mit Kaspersky Security Center gestartet werden soll:

- **MMC-basierte Verwaltungskonsole starten**
- **Kaspersky Security Center Web Console starten**

  Diese Option ist nur verfügbar, wenn Sie in einem der vorherigen Schritte Kaspersky Security Center Web Console installiert haben.

Sie können außerdem auf **Fertigstellen** klicken, um den Assistenten abzuschließen, ohne Kaspersky Security Center zu verwenden. Sie können später jederzeit mit der Verwendung des Programms beginnen.

Beim ersten Start der Verwaltungskonsole oder Kaspersky Security Center Web Console können Sie eine Erstkonfiguration des Programms ausführen.

Installation des Administrationsservers im Silent-Modus

Der Administrationsserver kann im Silent-Modus installiert werden, d. h. ohne die interaktive Eingabe von Installationseinstellungen.

Um den Administrationsservers im Silent-Modus auf einem lokalen Gerät zu installieren:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Verwenden Sie den unten angegebenen Befehl nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.
2. Lesen Sie die Datenschutzrichtlinie. Verwenden Sie den folgenden Befehl nur, wenn Sie verstehen und damit einverstanden sind, dass Ihre Daten, wie in der Datenschutzrichtlinie beschrieben, verarbeitet und übertragen werden (auch in Drittländer).

3. geben Sie folgenden Befehl ein:

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <Parameter>"
```

Dabei steht `Parameter` für Liste mit Einstellungen und Einstellungswerten, die durch Leerzeichen getrennt werden (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Die Datei setup.exe befindet sich im Ordner "Server" im Programmpaket von Kaspersky Security Center.

Die Namen und die möglichen Einstellungswerte, die bei der Installation des Administrationsservers im Silent-Modus zulässig sind, werden in folgender Tabelle angegeben.

Einstellungen für die Installation des Administrationsservers im Silent-Modus

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Lizenzvertrags.	• 1 – Ich habe die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen, und verstehe und akzeptiere sie. • Anderer Wert oder keine Angabe – die Bedingungen des Endbenutzer-Lizenzvertrags werden abgelehnt (die Installation wird nicht ausgeführt).
PRIVACYPOLICY	Einverständnis mit den Bedingungen der Datenschutzrichtlinie.	• 1 – Mir ist bewusst, dass meine Daten wie in der Datenschutzrichtlinie beschrieben verarbeitet und (einschließlich in Drittländer) übertragen werden. Ich bestätige, dass ich die Datenschutzrichtlinie vollständig gelesen habe und sie verstehe. • Anderer Wert oder keine Angabe – die Bedingungen der Datenschutzrichtlinie werden abgelehnt (die Installation wird nicht ausgeführt).
INSTALLATIONMODETYPE	Installationstyp für den Administrationsserver.	• Standard – standardmäßige Installation. • Custom – benutzerdefinierte Installation.
INSTALLDIR	Pfad des Installationsordners für den Administrationsserver	Zeichenfolgenwert.
ADDLOCAL	Liste der zur Installation vorgesehenen Komponenten (durch Komma getrennt) des Administrationsservers	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Liste der Komponenten, die als Mindestvoraussetzungen für eine korrekte Installation des Administrationsservers gelten: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.
NETRANGETYPE	Größe des Netzwerks (Anzahl der Geräte im Netzwerk)	• NRT_1_100 – von 1 bis 100 Geräte • NRT_100_1000 – von 101 bis 1.000 Geräte • NRT_GREATER_1000 – mehr als 1.000 Geräte
SRV_ACCOUNT_TYPE	Methode zum Erstellen eines Benutzerkontos, unter dem der Administrationsserver als Dienst gestartet wird	• SrvAccountDefault – Das Benutzerkonto wird automatisch erstellt. • SrvAccountUser – Das Benutzerkonto wird manuell erstellt. In diesem Fall müssen Werte für die Parameter `SERVERACCOUNTNAME` und `SERVERACCOUNTPWD` angegeben werden.
SERVERACCOUNTNAME	Benutzerkonto-Name, unter dem der Administrationsserver als Dienst gestartet wird. Der Parameterwert wird angegeben, wenn SRV_ACCOUNT_TYPE=SrvAccountUser.	Zeichenfolgenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
SERVERACCOUNTPWD	Kennwort des Benutzerkontos, unter dem der Administrationsserver als Dienst gestartet werden soll. Der Parameterwert wird angegeben, wenn SRV_ACCOUNT_TYPE=SrvAccountUser.	Zeichenfolgenwert.
SERVERCER	Die Lange des Schlüssels für das Zertifikat des Administrationsservers (in Bits).	• 1 – die Länge des Schlüssels für das Zertifikat des Administrationsservers beträgt 2048 Bit. • Kein Wert angegeben – die Länge des Schlüssels für das Zertifikat des Administrationsservers beträgt 1024 Bit.
DBTYPE	Typ der Datenbank, die zum Speichern der Informationsdatenbank des Administrationsservers verwendet wird. Dieser Parameter ist erforderlich.	• MySQL – Eine MySQL- oder MariaDB-Datenbank wird verwendet. In diesem Fall müssen Werte für die Parameter `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` und `MYSQLACCOUNTPWD` angegeben werden. • MSSQL – Eine Datenbank des Typs Microsoft SQL Server (SQL Express) wird verwendet. In diesem Fall müssen Werte für die Parameter `MSSQLSERVERNAME`, `MSSQLDBNAME`, `MSSQLAUTHTYPE` angegeben werden. • POSTGRES – Es wird eine PostgreSQL- oder Postgres Pro-Datenbank verwendet. In diesem Fall müssen die Werte für die Parameter `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` und `POSTGRESACCOUNTPWD` angegeben werden.
MYSQLSERVERNAME	Vollständiger Name des SQL-Servers. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MYSQLSERVERPORT	Portnummer für die Verbindung zum SQL-Server. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zahlenwert.
MYSQLDBNAME	Name der Datenbank, die erstellt wird, um Informationen des Administrationsservers zu speichern. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MYSQLACCOUNTNAME	Benutzerkonto-Name für die Verbindung mit der Datenbank. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MYSQLACCOUNTPWD	Kennwort des Benutzerkontos für die Verbindung zur Datenbank. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MSSQLSERVERNAME	Vollständiger Name des SQL-Servers. Der Parameterwert wird angegeben, wenn DBTYPE=MSSQL.	Zeichenfolgenwert.
MSSQLDBNAME	Name der Datenbank. Der Parameterwert wird angegeben, wenn DBTYPE=MSSQL.	Zeichenfolgenwert.
MSSQLAUTHTYPE	Autorisierungstyp für eine Verbindung mit dem SQL-Server. Der Parameterwert wird angegeben, wenn DBTYPE=MSSQL.	• Windows – Authentifizierungsmodus Microsoft Windows. • SQLServer – Authentifizierungsmodus für den SQL-Server. In diesem Fall müssen Werte für die Parameter `MSSQLACCOUNTNAME` und `MSSQLACCOUNTPWD` angegeben werden.
MSSQLACCOUNTNAME	Benutzerkonto-Name für die Verbindung zum SQL-Server. Der Parameterwert wird angegeben, wenn MSSQLAUTHTYPE=SQLServer.	Zeichenfolgenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
MSSQLACCOUNTPWD	Kennwort des Benutzerkontos für die Verbindung zum SQL-Server. Der Parameterwert wird angegeben, wenn MSSQLAUTHTYPE=SQLServer.	Zeichenfolgenwert.
CREATE_SHARE_TYPE	Methode zum Erstellen eines gemeinsamen Ordners.	• Create – neuen freigegebenen Ordner erstellen. In diesem Fall müssen Werte für die Parameter `SHARELOCALPATH` und `SHAREFOLDERNAME` angegeben werden. • ChooseExisting – Vorhandenen Ordner auswählen. In diesem Fall müssen Werte für den Parameter `EXISTSHAREFOLDERNAME` angegeben werden.
SHARELOCALPATH	Vollständiger Pfad eines lokalen Ordners. Der Parameterwert wird angegeben, wenn CREATE_SHARE_TYPE=Create	Zeichenfolgenwert.
SHAREFOLDERNAME	Netzwerkname des gemeinsamen Ordners. Der Parameterwert wird angegeben, wenn CREATE_SHARE_TYPE=Create	Zeichenfolgenwert.
EXISTSHAREFOLDERNAME	Vollständiger Name eines vorhandenen gemeinsamen Ordners. Der Parameterwert wird angegeben, wenn CREATE_SHARE_TYPE=ChooseExisting	Zeichenfolgenwert.
SERVERPORT	Portnummer für das Herstellen einer Verbindung mit dem Administrationsserver	Zahlenwert.
SERVERSSLPORT	Portnummer für das Herstellen einer sicheren Verbindung mit dem Administrationsserver über das SSL-Protokoll	Zahlenwert.
SERVERADDRESS	Adresse des Administrationsservers.	Zeichenfolgenwert.
MOBILESERVERADDRESS	Adresse des Administrationsservers für die Verbindung mit mobilen Geräten.	Zeichenfolgenwert.

Ausführliche Angaben über die Einstellungen für die Installation des Administrationsservers finden Sie im Abschnitt Benutzerdefinierte Installation.

Verwaltungskonsole auf dem Administrator-Arbeitsplatz installieren

Sie können die Verwaltungskonsole separat auf dem Administrator-Arbeitsplatz installieren und über diese Konsole den Administrationsserver verwalten.

Um die Verwaltungskonsole auf dem Administrator-Arbeitsplatz zu installieren, gehen Sie wie folgt vor:

1. Starten Sie die ausführbare Datei setup.exe.

   Ein Fenster wird geöffnet, in dem Sie Kaspersky-Anwendungen zur Installation auswählen können.

2. Klicken Sie im Fenster zur Programmauswahl auf den Link **Nur Kaspersky Security Center Verwaltungskonsole installieren**, um den Installationsassistenten der Verwaltungskonsole zu starten. Folgen Sie den Anweisungen des Assistenten.

3. Wählen Sie den Zielordner aus. Standardmäßig handelt es sich um <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center Console. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch bei der Installation angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** ändern.

4. Klicken Sie im letzten Fenster des Installationsassistenten auf die Schaltfläche **Beginnen**, um mit der Installation der Verwaltungskonsole zu beginnen.

Nach Abschluss des Assistenten wird die Verwaltungskonsole im Administrator-Arbeitsplatz installiert.

Um die Verwaltungskonsole auf dem Administrator-Arbeitsplatz im Silent-Modus zu installieren, gehen Sie wie folgt vor:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Verwenden Sie den unten angegebenen Befehl nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.

2. Führen Sie innerhalb des Vertriebspakets von Kaspersky Security Center im Ordner `Distrib\Console` die Datei "setup.exe" mit dem folgenden Befehl aus:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Wenn Sie sämtliche Verwaltungs-Plug-ins aus dem Ordner `Distrib\Console\Plugins` zusammen mit der Verwaltungskonsole installieren möchten, folgenden Befehl aus:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Wenn Sie bestimmte Verwaltungs-Plug-ins aus dem Ordner `Distrib\Console\Plugins` zusammen mit der Verwaltungskonsole installieren möchten, geben Sie die Plug-ins mithilfe des Parameters "/p" an und separieren Sie diese mit einem Semikolon:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   wobei `P1`, `P2`, `P3` für die Namen der Plug-ins steht, die mit den Ordnernamen innerhalb des Ordners `Distrib\Console\Plugins` übereinstimmen müssen. Beispiele:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

Die Verwaltungskonsole und Verwaltungs-Plug-ins (falls ausgewählt) werden auf dem Administrator-Arbeitsplatz installiert.

Nach Abschluss der Installation der Verwaltungskonsole muss eine Verbindung mit dem Administrationsserver hergestellt werden. Starten Sie dazu die Verwaltungskonsole und geben Sie im folgenden Fenster den Namen oder die IP-Adresse des Geräts, auf dem der Administrationsserver installiert ist, sowie die Benutzerkonto-Einstellungen für den Verbindungsaufbau an. Nachdem die Verbindung zum Administrationsserver hergestellt wurde, können Sie den Antiviren-Schutz über diese Verwaltungskonsole verwalten.

Sie können die Verwaltungskonsole mit den Standardmitteln zur Installation und Deinstallation von Microsoft Windows-Programmen deinstallieren.

Änderungen im System nach der Installation von Kaspersky Security Center

Icon der Verwaltungskonsole

Nachdem die Verwaltungskonsole auf Ihrem Gerät installiert wurde, wird ihr Symbol angezeigt, was Ihnen ermöglicht, die Verwaltungskonsole zu starten. Sie können die Verwaltungskonsole im Startmenü unter **Start → Programme → Kaspersky Security Center** finden.

Die Dienste des Administrationsservers und des Administrationsagenten

Der Administrationsserver und der Administrationsagent werden auf dem Gerät als Dienste mit den Eigenschaften installiert, die in der untenstehenden Tabelle aufgeführt sind. In der Tabelle werden auch Attribute anderer Dienste angezeigt, die auf dem Gerät nach der Installation des Administrationsservers ausgeführt werden.

Eigenschaften der Dienste von Kaspersky Security Center

Komponente	Name des Dienstes	Dargestellter Name des Dienstes	Benutzerkonto
Administrationsserver	kladminserver	Kaspersky Security Center Administrationsserver	Ein vom Benutzer angegebenes oder ein speziell bei der Installation erstelltes, nicht privilegiertes Benutzerkonto der Art KL-AK-*
Administrationsagent	klnagent	Kaspersky Security Center Administrationsagent	Lokales System
Webserver für den Zugriff auf Kaspersky Security Center Web Console und Verwaltung des Intranet des Unternehmens	klwebsrv	Web-Server von Kaspersky	Spezielles, nicht privilegiertes, Benutzerkonto KlScSvc
Aktivierungs-Proxyserver	klactprx	Aktivierungs-Proxy-Server von Kaspersky	Spezielles, nicht privilegiertes, Benutzerkonto KlScSvc
KSN-Proxyserver	ksnproxy	Proxyserver von Kaspersky Security Network	Spezielles, nicht privilegiertes, Benutzerkonto KlScSvc

Wenn Sie Kaspersky Security Center auf den Knoten eines Kaspersky Security Center Failover-Clusters installieren, wird der Dienst "klfocsvc_klfoc" verfügbar. Die Dienste "klnagent_klfoc" und "klfocsvc_klfoc" werden unter dem lokalen Systemkonto ausgeführt. Der Dienst "kladminserver_klfoc" muss unter dem Benutzerkonto "ksc" ausgeführt werden, und die weiteren Dienste müssen unter dem Benutzerkonto "rightless" ausgeführt werden. Die Benutzerkonten "ksc" und "rightless" müssen der Gruppe "KLAdmins" mit den Berechtigungen eines lokalen Administrators hinzugefügt werden. Damit Kaspersky Security Center ordnungsgemäß ausgeführt wird, dürfen Sie zum Ausführen der Dienste nur die Benutzerkonten "ksc" und "rightless" verwenden. Es wird nicht empfohlen, andere Konten mit denselben Rechten zu verwenden. Die folgende Tabelle enthält die Eigenschaften der Dienste, die nach der Installation des Administrationsservers auf dem Kaspersky Security Center Failover-Cluster auf dem Gerät angewendet werden.

Eigenschaften der Dienste des auf dem Kaspersky Security Center Failover-Cluster installierten Kaspersky Security Centers

Komponente	Name des Dienstes	Dargestellter Name des Dienstes	Benutzerkonto
Administrationsserver	kladminserver_klfoc	Kaspersky Security Center Administrationsserver	ksc
Administrationsagent	klnagent_klfoc	Kaspersky Security Center Administrationsagent	Lokales System
Webserver für den Zugriff auf Kaspersky Security Center Web Console und Verwaltung des Intranet des Unternehmens	klwebsrv_klfoc	Web-Server von Kaspersky	rightless

Aktivierungs-Proxyserver	klactprx_klfoc	Aktivierungs-Proxy-Server von Kaspersky	rightless
KSN-Proxyserver	ksnproxy_klfoc	Proxyserver von Kaspersky Security Network	rightless
Kaspersky Security Center Failover-Cluster	klfocsvc_klfoc	Kaspersky Security Center Failover-Cluster	Lokales System

Dienste der Kaspersky Security Center Web Console

Wenn Sie Kaspersky Security Center Web Console auf dem Gerät installieren, werden die folgenden Dienste bereitgestellt (siehe untere Tabelle):

Dienste der Kaspersky Security Center Web Console

Dargestellter Name des Dienstes	Benutzerkonto
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	Netzwerkdienst
Kaspersky Security Center Server für Produkt-Plug-ins	NT Service/KSCWebConsolePlugin
Verwaltungsdienst der Kaspersky Security Center Web Console	Lokales System
Nachrichten-Warteschlange von Kaspersky Security Center Web Console	NT Service/KSCWebConsoleMessageQueue

Server-Version des Administrationsagenten

Zusammen mit dem Administrationsserver wird auf dem Gerät die Serverversion des Administrationsagenten installiert. Die Serverversion des Administrationsagenten gehört zum Administrationsserver, wird mit ihm installiert oder deinstalliert und kann nur mit dem lokal installierten Administrationsserver zusammenarbeiten. Sie müssen die Verbindung des Administrationsagenten mit dem Administrationsserver nicht anpassen: die Konfiguration wird programmseitig implementiert, da die Komponenten auf demselben Gerät installiert werden. Die Serverversion des Administrationsagenten wird mit den gleichen Attributen installiert und erfüllt die gleichen Programmverwaltungsfunktionen wie der standardmäßige Administrationsagent. Diese Version wird durch die Richtlinie der Administrationsgruppe verwaltet, zu welcher das Client-Gerät des Administrationsservers gehört. Für die Serverversion des Administrationsagenten werden alle Aufgaben erstellt, die für den Administrationsserver vorgesehen sind (ausgenommen Aufgabe zum Wechsel des Servers).

Eine separate Installation des Administrationsagenten auf dem Gerät mit dem Administrationsserver ist unmöglich.

Sie können die Eigenschaften der Dienste des Administrationsservers und des Administrationsagenten anzeigen und deren Ausführung mithilfe der standardmäßigen Administrationsmitteln von Microsoft Windows Computerverwaltung\Dienste verfolgen. Informationen über die Aktivität des Kaspersky-Administrationsserver-Dienstes werden im Microsoft Windows-Systemprotokoll in einem separaten Zweig namens Kaspersky-Ereignisprotokoll auf dem Gerät gespeichert, auf dem der Administrationsserver installiert ist.

Es wird nicht empfohlen, die Dienste manuell zu starten und zu beenden bzw. die Benutzerkonten in den Einstellungen der Dienste zu verändern. Falls notwendig, können Sie das Benutzerkonto für den Dienst des Administrationsservers mithilfe des Tools klsrvswch tauschen. Beachten Sie, dass Sie das Tool "klsrvswch" auf dem Administrationsserver unter dem Benutzerkonto mit Administratorrechten starten müssen, das für die Installation des Administrationsservers verwendet wurde.

Benutzerkonten und Sicherheitsgruppen

Der Installer des Administrationsservers erstellt standardmäßig folgende Benutzerkonten:

- KL-AK-*: Benutzerkonto für Dienst des Administrationsservers.
- KlScSvc: Benutzerkonto für die übrigen Dienste aus dem Bestand des Administrationsservers.
- KlPxeUser: Benutzerkonto für die Bereitstellung des Betriebssystems.

Wenn Sie während der Ausführung des Installers andere Benutzerkonten für die Dienste des Administrationsservers und weitere Dienste ausgewählt haben, werden die von Ihnen angegebenen Benutzerkonten verwendet.

Auf dem Gerät, auf dem der Administrationsserver installiert ist, werden außerdem automatisch die lokalen Sicherheitsgruppen KLAdmins und KLOperators mir ihren entsprechenden Berechtigungen angelegt.

Es wird nicht empfohlen, den Administrationsserver auf einem Domänencontroller zu installieren. Wenn Sie den Administrationsserver dennoch auf dem Domänencontroller installieren, müssen Sie das Installationsprogramm mit den Domänen-Administratorrechten starten. In diesem Fall erstellt das Installationsprogramm automatisch Domänen-Sicherheitsgruppen mit den Namen KLAdmins und KLOperators. Wenn Sie den Administrationsserver auf einem Gerät installieren, das nicht der Domänencontroller ist, müssen Sie das Installationsprogramm mit den lokalen Administratorrechten starten. In diesem Fall erstellt das Installationsprogramm automatisch lokale Sicherheitsgruppen mit den Namen KLAdmins und KLOperators.

Bei der Konfiguration der E-Mail-Benachrichtigungen kann es erforderlich sein, ein Benutzerkonto auf einem Mail-Server für die ESMTP-Authentifizierung einzurichten.

Programmdeinstallation

Sie können Kaspersky Security Center mit den Standardmitteln zur Installation und Deinstallation von Microsoft Windows-Programmen entfernen. Zur Deinstallation des Programms wird der Assistent gestartet, durch den alle Programmkomponenten (mit Plug-ins) vom Gerät deinstalliert werden. Der Assistent öffnet in Ihren Standardbrowser eine Webseite mit einer Umfrage, auf der Sie uns mitteilen können, warum Sie sich entschieden haben, Kaspersky Security Center nicht mehr zu verwenden. Wenn Sie in dem Assistenten nicht angegeben haben, dass der gemeinsame Ordner (KLSHARE) deinstalliert werden soll, können Sie ihn nach Abschluss aller entsprechenden Aufgaben manuell deinstallieren.

Nach der Deinstallation des Programms können sich noch immer Dateien im temporären Systemordner befinden.

Der Assistent für das Erstellen einer Aufgabe zur Deinstallation eines Programms schlägt Ihnen vor, eine Backup-Kopie der Daten des Administrationsservers zu speichern.

Bei der Deinstallation von Anwendungen von Computern mit dem Betriebssystem Microsoft Windows 7 oder Microsoft Windows 2008 ist ein vorzeitiges Beenden des Assistenten für das Erstellen einer Aufgabe zur Deinstallation eines Programms möglich. Um dies zu verhindern, deaktivieren Sie im Betriebssystem die Benutzerkontensteuerung (UAC) und starten die Deinstallation des Programms erneut.

Über das Upgrade von Kaspersky Security Center

Dieser Abschnitt enthält Informationen darüber, wie ein Upgrade von einer vorherigen Version von Kaspersky Security Center ausgeführt werden kann. Sie können das Upgrade von Kaspersky Security Center auf verschiedene Arten durchführen, je nachdem, ob Kaspersky Security Center lokal oder auf den Knoten eines Kaspersky Security Center Failover-Clusters installiert wurde.

Während des Upgrades ist unbedingt darauf zu achten, dass keine gemeinsame Nutzung des DBMS durch den Administrationsserver und einer anderen Anwendung stattfindet.

Beachten Sie, dass Sie bei einer Aktualisierung des Administrationsservers auf Version 15.1 keine neuen Installationspakete des Administrationsagenten in Version 15 oder früher erstellen können. Bereits zuvor erstellte Installationspakete bleiben jedoch verfügbar.

Wenn Sie das Upgrade von Kaspersky Security Center von einer älteren Version durchführen, werden alle installierten Plug-ins für unterstützte Kaspersky-Anwendungen beibehalten. Das Upgrade für das Plug-in des Administrationsservers und das Plug-in des Administrationsagenten erfolgt automatisch (sowohl für die Verwaltungskonsole als auch für Kaspersky Security Center Web Console).

Update der vorherigen Version von Kaspersky Security Center

Der folgende Artikel beschreibt die empfohlenen Schritte für die Vorbereitung des Upgrades: Upgrades von Kaspersky Security Center und der verwalteten Sicherheitsanwendungen.

Sie können Version 15.1 des Administrationsservers auf einem Gerät installieren, auf dem eine ältere Version des Administrationsservers installiert ist (ab Version 11 (11.0.0.1131b)). Beim Aktualisieren auf die Version 15.1 bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Sollten bei der Installation des Administrationsservers Probleme auftreten, können Sie die vorherige Version des Administrationsservers wiederherstellen, indem Sie die vor dem Update erstellte Backup-Kopie der Serverdaten heranziehen.

Wenn im Netzwerk mindestens ein Administrationsserver der neuen Version installiert ist, können Sie die anderen Administrationsserver im Netzwerk mithilfe der Aufgabe zur Remote-Installation installieren, in welcher das Installationspaket des Administrationsservers verwendet wird.

Wenn Sie das Kaspersky Security Center auf dem Failover-Cluster bereitgestellt haben, können Sie auch Kaspersky Security Center auf den Knoten aktualisieren.

Um den Administrationsserver von der vorhergehenden Version auf die Version 15.1 zu aktualisieren, gehen Sie wie folgt vor:

1. Starten Sie die Installationsdatei ksc_15.1_<Build-Nummer>_full_<Sprachversion>.exe für Version 15.1 (diese Datei können Sie von der Kaspersky-Website herunterladen).

2. Klicken Sie im angezeigten Fenster auf den Link **Kaspersky Security Center installieren**, um den Installationsassistenten des Administrationsservers zu starten. Folgen Sie den Anweisungen des Assistenten.

3. Lesen Sie sich den Lizenzvertrag und die Datenschutzrichtlinie sorgfältig durch. Wenn Sie mit allen Punkten des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie im Block **Ich bestätige die vollständige Kenntnis, das Verständnis und das Einverständnis bezüglich** die Kontrollkästchen:

   - **Den Bestimmungen und Bedingungen dieser EULA**
   - **Der Datenschutzrichtlinie, in der die Datenverarbeitung beschrieben wird**

   Die Programminstallation wird nach dem Aktivieren beider Kontrollkästchen fortgesetzt. Der Installationsassistent fordert Sie auf, ein Backup der Daten des Administrationsservers für die ältere Version zu erstellen.

   Kaspersky Security Center unterstützt die Datenwiederherstellung aus einem Backup, das mit einer älteren Version des Administrationsservers erstellt wurde.

4. Wenn Sie ein Backup der Daten des Administrationsservers erstellen möchten, geben Sie dies im angezeigten Fenster **Backup der Daten des Administrationsservers anlegen** an.

   Ein Backup wird vom Dienstprogramm klbackup erstellt. Das Tool gehört zum Programmpaket und wird im Stammverzeichnis der Installation von Kaspersky Security Center abgelegt.

5. Installieren Sie den Administrationsserver in Version 15.1. Indem Sie dazu den Anweisungen des Installationsassistenten folgen.

   Sollte eine Meldung darüber angezeigt werden, dass der Dienst von Kaspersky Security Center Web Console ausgelastet ist, klicken Sie im Fenster des Assistenten auf **Ignorieren**.

   Es wird nicht empfohlen, die Ausführung des Installationsassistenten abzubrechen. Wenn Sie das Upgrade während der Installation des Administrationsservers abbrechen, ist die aktualisierte Version von Kaspersky Security Center möglicherweise funktionsunfähig.

6. Für die Geräte, auf denen die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

   Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center.

   Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

Führen Sie die folgenden Befehle auf Linux-basierten Assets aus, um nicht mehr benötigte Abhängigkeiten zu entfernen:

- Führen Sie für Debian-basierte Assets einen der folgenden Befehle aus:
  - `apt-get -y autoremove`
  - `apt -y autoremove`
- Führen Sie für RPM-basierte Assets einen der folgenden Befehle aus:
  - `dnf autoremove`
  - `yum autoremove`

Kaspersky Security Center auf den Knoten des Kaspersky Security Center Failover-Clusters aktualisieren

Sie können den Administrationsserver in Version 15.1 auf jedem Knoten des Kaspersky Security Center Failover-Clusters installieren, auf dem der Administrationsserver in einer früheren Version installiert ist (beginnend mit Version 13.2). Beim Aktualisieren auf die Version 15.1 bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Wenn Sie Kaspersky Security Center bereits früher lokal auf Geräten installiert haben, können Sie auf diesen Geräten ebenfalls ein Upgrade von Kaspersky Security Center durchführen.

So aktualisieren Sie Kaspersky Security Center auf den Knoten des Kaspersky Security Center Failover-Clusters:

1. Führen Sie auf dem aktiven Knoten des Clusters folgende Vorgänge aus:
   a. Starten Sie die ausführbare Datei "ksc_15.1_<Build Nummer>_full_<Sprache>.exe".

      Es wird ein Fenster geöffnet, in dem Sie die Kaspersky-Anwendungen auswählen müssen, die ein Upgrade erhalten sollen. Klicken Sie auf den Link **Kaspersky Security Center Administrationsserver installieren**, um den Installationsassistenten des Administrationsservers zu starten. Folgen Sie den Anweisungen des Assistenten.

   b. Lesen Sie sich den Lizenzvertrag und die Datenschutzrichtlinie sorgfältig durch. Wenn Sie mit allen Punkten des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie im Block **Ich bestätige die vollständige Kenntnis, das Verständnis und das Einverständnis bezüglich** die Kontrollkästchen:
      - **Den Bestimmungen und Bedingungen dieser EULA**
      - **Der Datenschutzrichtlinie, in der die Datenverarbeitung beschrieben wird**

      Aktivieren Sie beide Kontrollkästchen, um die Installation fortzusetzen.

      Wenn Sie den Lizenzvertrag und die Datenschutzrichtlinie nicht akzeptieren, klicken Sie auf die Schaltfläche **Abbrechen**, um das Upgrade abzubrechen.

2. Führen Sie auf dem passiven Knoten des Kaspersky Security Center Failover-Clusters dieselben Vorgänge aus wie auf dem aktiven Knoten.

3. Starten Sie das Cluster.

Anschließend haben Sie die neuste Version des Administrationsservers auf den Knoten des Kaspersky Security Center Failover-Clusters installiert.

Kaspersky Security Center auf den Knoten eines Microsoft-Failover-Clusters aktualisieren

Sie können den Administrationsserver in Version 15.1 auf jedem Knoten des Microsoft-Failover-Clusters aktualisieren, auf dem der Administrationsserver in einer früheren Version installiert ist (beginnend mit Version 13.2). Beim Aktualisieren auf die Version 15.1 bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Um Kaspersky Security Center auf den Knoten des Microsoft-Failover-Clusters zu aktualisieren, führen Sie die folgenden Schritte auf einem beliebigen Knoten des Clusters aus:

1. Starten Sie die ausführbare Datei "ksc_15.1_<Build Nummer>_full_<Sprache>.exe".

   Es wird ein Fenster geöffnet, in dem Sie die Kaspersky-Anwendungen auswählen müssen, die ein Upgrade erhalten sollen. Klicken Sie auf den Link **Kaspersky Security Center Administrationsserver installieren**, um den Installationsassistenten des Administrationsservers zu starten. Folgen Sie den Anweisungen des Assistenten.

2. Lesen Sie sich den Lizenzvertrag und die Datenschutzrichtlinie sorgfältig durch. Wenn Sie mit allen Punkten des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie im Block **Ich bestätige die vollständige Kenntnis, das Verständnis und das Einverständnis bezüglich** die Kontrollkästchen:

   - **Den Bestimmungen und Bedingungen dieser EULA**
   - **Der Datenschutzrichtlinie, in der die Datenverarbeitung beschrieben wird**

   Aktivieren Sie beide Kontrollkästchen, um die Installation fortzusetzen.

   Wenn Sie den Lizenzvertrag und die Datenschutzrichtlinie nicht akzeptieren, klicken Sie auf die Schaltfläche **Abbrechen**, um das Upgrade abzubrechen.

3. Wählen Sie im Fenster **Installationstyp für Cluster** die Option **Cluster (auf allen Cluster-Knoten installieren)** aus.

   Anschließend konfiguriert das Installationsprogramm den Administrationsserver auf allen Knoten des Clusters und schließt das Upgrade ab. Während des Upgrades können die Einstellungen des Administrationsservers nicht geändert werden.

Als Ergebnis haben Sie die neuste Version des Administrationsservers auf den Knoten des Microsoft-Failover-Clusters installiert.

Erstkonfiguration von Kaspersky Security Center

In diesem Abschnitt werden die Schritte beschrieben, die Sie nach der Installation von Kaspersky Security Center zur Ersteinrichtung des Programms ausführen müssen.

Leitfaden zur Härtung

Der Härtungsleitfaden richtet sich an Experten, die für die Installation und Administration von Kaspersky Security Center zuständig sind, sowie an Experten, die für den technischen Support von Unternehmen verantwortlich sind, die Kaspersky Security Center einsetzen.

Der Härtungsleitfaden beschreibt Empfehlungen und Funktionen zur Konfiguration von Kaspersky Security Center und seinen Komponenten, mit dem Ziel, das Risiko einer Kompromittierung zu verringern.

Erstellen Sie vor der Konfiguration eine Backup-Kopie des Kaspersky Security Center Administrationsservers mittels der Aufgabe Backup der Daten des Administrationsservers anlegen oder des Tools "klbackup" und speichern Sie sie an einem sicheren Ort.

Der Härtungsleitfaden enthält die folgenden Informationen:

- Auswahl der Administrationsserver-Architektur
- Konfigurieren einer sicheren Verbindung zum Administrationsserver
- Konfigurieren der Benutzerkonten, um auf den Administrationsserver zuzugreifen
- Verwaltung des Schutzes des Administrationsservers und der Client-Geräte
- Konfigurieren des Schutzes für verwaltete Programme
- Wartung des Administrationsservers
- Übertragen von Informationen an Programme von Drittanbietern

Bevor Sie mit dem Administrationsserver arbeiten, fordert Kaspersky Security Center Sie auf, die Kurzfassung des Härtungsleitfadens zu lesen.

Beachten Sie, dass Sie den Administrationsserver erst verwenden können, nachdem Sie bestätigt haben, dass Sie den Härtungsleitfaden gelesen haben.

So lesen Sie den Härtungsleitfaden:

1. Öffnen Sie die Verwaltungskonsole oder die Kaspersky Security Center Web Console und melden Sie sich an der Konsole an. Die Konsole prüft, ob Sie das Lesen der aktuellen Version des Härtungsleitfaden bestätigt haben.

   Wenn Sie den Härtungsleitfaden noch nicht gelesen haben, öffnet sich ein Fenster und zeigt eine Kurzfassung davon an.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Kurzfassung des Härtungsleitfadens als Textdokument anzeigen möchten, klicken Sie auf den Link **In neuem Fenster öffnen**.

   - Wenn Sie vollständige Fassung des Härtungsleitfadens anzeigen möchten, klicken Sie auf den Link **Härtungsleitfaden in der Online-Hilfe öffnen** anzeigen.

3. Nachdem Sie den Härtungsleitfaden gelesen haben, aktivieren Sie das Kontrollkästchen **Ich bestätige, dass ich den Härtungsleitfaden vollständig gelesen habe und ihn verstehe** und klicken Sie anschließend auf die Schaltfläche **Akzeptieren**.

Sie können jetzt mit dem Administrationsserver arbeiten.

Wenn eine neue Version des Härtungsleitfadens veröffentlicht wird, werden Sie von Kaspersky Security Center dazu aufgefordert, diese zu lesen.

Der Schnellstartassistent für den Administrationsserver

Dieser Abschnitt enthält Informationen zum Schnellstartassistenten für den Administrationsserver.

Über den Schnellstartassistenten

Dieser Abschnitt enthält Informationen zum Schnellstartassistenten für den Administrationsserver.

Im Schnellstartassistenten für den Administrationsserver können Sie die minimal erforderlichen Aufgaben und Richtlinien erstellen, eine Mindestauswahl an Einstellungen anpassen, Plug-ins für verwaltete Kaspersky-Anwendungen herunterladen und installieren, und Installationspakete für verwaltete Kaspersky-Anwendungen erstellen. Während der Ausführung des Assistenten können Sie die folgenden Änderungen am Programm vornehmen:

- Plug-ins für verwaltete Programme herunterladen und installieren. Nach Abschluss des Schnellstartassistenten wird die Liste der installierten Verwaltungs-Plug-ins im Abschnitt **Erweitert → Informationen über installierte Programmverwaltungs-Plug-Ins** des Administrationsserver-Eigenschaftenfensters angezeigt.

- Installationspakete für verwaltete Kaspersky-Anwendungen erstellen. Nachdem der Schnellstartassistent abgeschlossen wurde, werden die Installationspakete des Administrationsagenten für Windows und für verwaltete Kaspersky-Anwendungen in der Liste **Administrationsserver → Erweitert → Remote-Installation → Installationspakete** angezeigt.

- Schlüsseldateien hinzufügen oder Aktivierungscodes eingeben, die automatisch auf die Geräte der Administrationsgruppen verteilt werden können. Nach Abschluss des Schnellstartassistenten werden Informationen über die Lizenzschlüssel in der Liste **Administrationsserver → Lizenzen für Kaspersky-Software** und im Abschnitt **Lizenzschlüssel** des Administrationsserver-Eigenschaftenfensters angezeigt.

- Interaktion mit Kaspersky Security Network (KSN) konfigurieren.

- E-Mail-Versand von Benachrichtigungen über Ereignisse konfigurieren, die vom Administrationsserver und den verwalteten Programmen registriert werden. (Damit Benachrichtigungen erfolgreich zugestellt werden, muss auf dem Administrationsserver und auf allen Geräten der Windows Messenger Dienst gestartet werden.) Nach Abschluss des Schnellstartassistenten werden die Einstellungen für E-Mail-Benachrichtigungen im Abschnitt **Benachrichtigung** des Administrationsserver-Eigenschaftenfensters angezeigt.

- Die Einstellungen für das Update und das Schließen von Schwachstellen der auf den Geräten installierten Programme anpassen.

- Schutzrichtlinien für Arbeitsstationen und Server sowie Aufgaben zur Schadsoftware-Untersuchung, Update-Download und Verschieben ins Backup für die oberste Hierarchieebene der verwalteten Geräte erstellen. Nach Abschluss des Schnellstartassistenten werden die erstellten Aufgaben in der Liste **Administrationsserver** → **Aufgaben** angezeigt. Die Richtlinien, die den Plug-ins für verwaltete Anwendungen entsprechen, werden in der Liste **Administrationsserver** → **Richtlinien** angezeigt.

Der Schnellstartassistent erstellt Richtlinien für verwaltete Programme, wie beispielsweise Kaspersky Endpoint Security für Windows, es sei denn, diese Richtlinien wurden bereits für die Gruppe **Verwaltete Geräte** erstellt. Der Schnellstartassistent erstellt Aufgaben, wenn für die Gruppe **Verwaltete Geräte** keine Aufgaben mit den gleichen Namen vorhanden sind.

Kaspersky Security Center fordert Sie in der Verwaltungskonsole automatisch zur Ausführung des Schnellstartassistenten auf, nachdem Sie das Programm zum ersten Mal gestartet haben. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

Start des Schnellstartassistenten für den Administrationsserver

Das Programm schlägt automatisch vor, beim ersten Verbindungsaufbau zum Server nach der Installation des Administrationsservers den Schnellstartassistenten zu starten. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

So starten Sie den Schnellstartassistenten manuell:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.

2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **Alle Aufgaben** → **Schnellstartassistent für den Administrationsserver**.

   Der Assistent schlägt vor, die ursprünglichen Einstellungen des Administrationsservers zu generieren. Folgen Sie den Anweisungen des Assistenten.

Wenn Sie den Schnellstartassistenten erneut ausführen, können die Aufgaben und Richtlinien, die bei der vorherigen Ausführung des Assistenten erstellt wurden, nicht neu erstellt werden.

Schritt 1. Konfigurieren eines Proxyservers

Geben Sie die Internetzugriffseinstellungen für den Administrationsserver an. Sie müssen den Internetzugang anpassen, um Kaspersky Security Network zu verwenden und um Updates für die Antiviren-Datenbanken von Kaspersky Security Center und die verwalteten Kaspersky-Anwendungen herunterzuladen.

Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

- **Adresse**

  Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center mit dem Internet.

- **Port**

  Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center hergestellt wird.

- **Proxyserver für lokale Adressen umgehen**

  Bei der Verbindung mit den Geräten im lokalen Netzwerk wird kein Proxyserver verwendet.

- **Authentifizierung am Proxyserver**

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver verwenden** aktiviert ist.

- **Benutzername**

  Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

- **Kennwort**

  Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

  Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

Das Konfigurieren des Internetzugriffs ist auch später, unabhängig vom Schnellstartassistenten, möglich.

Schritt 2. Auswählen der Methode zur Programmaktivierung

Wählen Sie eine der folgenden Varianten der Aktivierung von Kaspersky Security Center aus:

- **Durch Eingabe Ihres Aktivierungscodes**

  Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus 20 Buchstaben und Ziffern. Den Aktivierungscode geben Sie ein, um einen Schlüssel zur Aktivierung von Kaspersky Security Center hinzuzufügen. Sie erhalten den Aktivierungscode an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center angegeben haben.

  Um das Programm unter Verwendung eines Aktivierungscodes zu aktivieren, ist ein Internetzugang für die Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

  Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

  Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

  Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Knoten **Lizenzen für Kaspersky-Software** der Verwaltungskonsolenstruktur an die verwalteten Geräte verteilen.

  > Sollte die Aktivierung anhand Ihres eingegebenen Aktivierungscodes nicht erfolgreich verlaufen, können Sie die Anwendung auch durch das Angeben einer Schlüsseldatei aktivieren.

- **Durch Angabe einer Schlüsseldatei**

  Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Die Schlüsseldatei dient dazu, einen Schlüssel für die Aktivierung der Anwendung hinzuzufügen.

  Die Möglichkeiten zum Abrufen einer Schlüsseldatei werden im Abschnitt Über die Schlüsseldatei beschrieben.

Um das Programm mit einer Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Knoten **Lizenzen für Kaspersky-Software** der Verwaltungskonsolenstruktur an die verwalteten Geräte verteilen.

- **Durch ein Aufschieben der Anwendungsaktivierung**

  In diesem Fall wird die Anwendung mit grundlegenden Funktionen ausgeführt. Die Komponente "Verwaltung mobiler Geräte" und das Schwachstellen- und Patch-Management können jedoch nicht verwendet werden.

Falls Sie die Aktivierung der Anwendung aufschieben möchten, können Sie jederzeit später einen Lizenzschlüssel hinzufügen.

Schritt 3. Auswählen der Schutzbereiche und Betriebssysteme

Wählen Sie die Schutzbereiche und Betriebssysteme aus, die Sie in Ihrem Netzwerk verwenden. Geben Sie bei der Auswahl die Filter für die Plug-ins zur Anwendungsverwaltung und für die Programmpakete auf den Kaspersky-Servern an, die Sie herunterladen und auf Client-Geräten in Ihrem Netzwerk installieren können. Wählen Sie die Optionen aus:

- **Bereiche**

  Sie können die folgenden Schutzbereiche auswählen:

  - **Workstations**. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk Workstations schützen möchten. Standardmäßig ist die Variante "Workstations" ausgewählt.
  - **Dateiserver und Datenspeicherungssysteme**. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk Dateiserver schützen möchten.
  - **Mobile Geräte**. Wählen Sie diese Option aus, wenn Sie mobile Geräte schützen möchten, die dem Unternehmen oder den Unternehmensmitarbeitern gehören. Wenn Sie diese Option auswählen, aber keine Lizenz für die Funktion "Verwaltung mobiler Geräte" bereitgestellt haben, wird gemeldet, dass eine Lizenz mit der Funktion "Verwaltung mobiler Geräte" bereitgestellt werden muss. Wenn Sie keine Lizenz bereitstellen, können Sie die Funktion "Verwaltung mobiler Geräte" nicht verwenden.
  - **Virtualisierungen**. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk virtuelle Maschinen schützen möchten.
  - **Kaspersky Anti-Spam**. Wählen Sie diese Option aus, wenn Sie die Mail-Server Ihres Unternehmens vor Spam, Betrug und Schadsoftware schützen möchten.

- **Betriebssysteme**

  Sie können die folgende Plattformen auswählen:

  - Microsoft Windows
  - Linux
  - macOS

- Android
- Anderes

Informationen zu den unterstützten Betriebssystemen finden Sie in den Hard- und Softwarevoraussetzungen.

Das Auswählen der Pakete der Kaspersky-Anwendungen aus der Liste der verfügbaren Pakete kann später unabhängig vom Schnellstartassistenten durchgeführt werden. Um die Suche nach den benötigten Paketen zu vereinfachen, können Sie die Liste der verfügbaren Pakete nach folgenden Kriterien filtern:

- Schutzbereich
- Art der heruntergeladenen Software (Programmpaket, Tool, Plug-in oder Web-Plug-in)
- Version der Kaspersky-Anwendung
- Lokalisierungssprache der Kaspersky-Anwendung

Schritt 4. Auswählen der Plug-ins für verwaltete Programme

Auswahl der zu installierenden Plug-ins für verwaltete Anwendungen. Eine Liste aller auf Kaspersky-Servern befindlichen Plug-ins wird angezeigt. Die Liste wird nach den Optionen gefiltert, die beim vorherigen Schritt des Assistenten ausgewählt wurden. Standardmäßig enthält eine komplette Liste Plug-ins aller Sprachen. Um nur die Plug-ins einer bestimmten Sprache anzuzeigen, wählen Sie die Sprache aus der Dropdown-Liste **Anzeige der Sprache der Verwaltungskonsole oder**. Die Liste der Plug-ins umfasst die folgenden Spalten:

- **Programmname**

  Die Auswahl der Plug-ins richtet sich nach den Schutzbereichen und Plattformen, die Sie beim vorhergehenden Schritt ausgewählt haben.

- **Programmversion**

  Die Liste enthält Plug-ins aller auf Kaspersky-Servern befindlichen Versionen. Standardmäßig sind die Plug-ins der aktuellsten Versionen ausgewählt.

- **Lokalisierungssprache**

  Standardmäßig wird die Lokalisierungssprache eines Plug-ins durch die Sprache von Kaspersky Security Center vorgegeben, die Sie während der Installation ausgewählt haben. In der Dropdown-Liste **Anzeige der Sprache der Verwaltungskonsole oder** können Sie andere Sprachen angeben.

Nachdem die Plug-ins ausgewählt wurden, startet deren Installation in einem separaten Fenster automatisch. Für die Installation einiger Plug-ins müssen Sie die Bestimmungen der EULA akzeptierten. Lesen Sie den EULA-Text, aktivieren Sie die Option **Ich akzeptiere die Bestimmungen des Lizenzvertrages** und klicken Sie auf die Schaltfläche **Installieren**. Wenn Sie die Bestimmungen der EULA nicht akzeptieren, wird das Plug-in nicht installiert.

Schließen Sie das Installationsfenster nach dem Abschluss der Installation.

Sie können die Verwaltungs-Plug-Ins auch später auswählen, unabhängig vom Schnellstartassistenten.

Schritt 5. Herunterladen der Programmpakete Erstellen der Installationspakete

Kaspersky Endpoint Security für Windows enthält Verschlüsselungs-Tools für die Informationen, die auf Client-Geräten gespeichert werden. Um ein Programmpaket von Kaspersky Endpoint Security für Windows herunterzuladen, dass den Bedürfnissen Ihrer Organisation entspricht, konsultieren Sie die Gesetzgebung in dem Land, in dem sich die Client-Geräte Ihrer Organisation befinden.

Wählen Sie im Fenster **Verschlüsselungstyp** einen der folgenden Verschlüsselungs-Typen aus:

- Starke Verschlüsselung (AES256). Dieser Verschlüsselungstyp verwendet die 256-Bit-Schlüssellänge.
- Leichte Verschlüsselung (AES56). Dieser Verschlüsselungstyp verwendet die 56-Bit-Schlüssellänge.

Das Fenster **Verschlüsselungstyp** wird nur angezeigt, wenn Sie **Workstations** als einen Schutzbereich und **Microsoft Windows** als eine Plattform ausgewählt haben.

Nachdem Sie einen Verschlüsselungstyp ausgewählt haben, wird eine Liste der Programmpakete für beide Verschlüsselungstypen angezeigt. In der Liste ist ein Programmpaket mit dem ausgewählten Verschlüsselungstyp ausgewählt. Die Sprache des Programmpakets entspricht der Sprache von Kaspersky Security Center. Wenn ein Programmpaket von Kaspersky Endpoint Security für Windows nicht in der Sprache von Kaspersky Security Center verfügbar ist, wird das englische Programmpaket ausgewählt.

Die Sprachen der Programmpakete können Sie in der Dropdown-Liste **Anzeige der Sprache der Verwaltungskonsole oder** auswählen.

Für Pakete verwalteter Programme muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center installiert werden.

In der Liste können Sie Programmpakete eines jeden Verschlüsselungs-Typs auswählen, unabhängig davon, welchen Typ Sie im Fenster **Verschlüsselungstyp** angegeben haben. Nachdem Sie ein Programmpaket für Kaspersky Endpoint Security für Windows ausgewählt haben, wird unter Berücksichtigung der Komponenten und Plattformen der Download der Programmpakete gestartet. Sie können den Download-Fortschritt in der Spalte **Download-Status** verfolgen. Nachdem der Schnellstartassistent abgeschlossen wurde, werden die Installationspakete des Administrationsagenten für Windows und für verwaltete Kaspersky-Programme in der Liste **Administrationsserver** → **Erweitert** → **Remote-Installation** → **Installationspakete** angezeigt.

Um den Download einiger Programmpakete abzuschließen, müssen Sie die EULA akzeptieren. Wenn Sie auf die Schaltfläche **Akzeptieren** klicken, wird der EULA-Text angezeigt. Um zum nächsten Schritt des Assistenten zu wechseln, müssen Sie die Bestimmungen und Bedingungen der EULA und die Bestimmungen und Bedingungen der Kaspersky-Datenschutzrichtlinie akzeptieren. Aktivieren Sie die Optionen hinsichtlich der EULA und der Datenschutzrichtlinie von Kaspersky und klicken Sie anschließend auf die Schaltfläche **Alle akzeptieren**. Wenn Sie die Bestimmungen und Bedingungen nicht akzeptieren, wird der Download des Pakets abgebrochen.

Nachdem Sie die Bestimmungen und Bedingungen der EULA und die Bestimmungen und Bedingungen der Kaspersky-Datenschutzrichtlinie akzeptiert haben, wird der Download des Programmpakets fortgesetzt. Wenn der Download abgeschlossen ist, wird der Status **Das Installationspaket wurde erstellt** angezeigt. Die Installationspakete können Sie später verwenden, um Kaspersky-Anwendungen auf Client-Geräten bereitzustellen.

Das Erstellen der Installationspakete kann manuell, unabhängig vom Schnellstartassistenten, durchgeführt werden. Wechseln Sie in der Baumstruktur der Verwaltungskonsole zu **Administrationsserver** → **Erweitert** → **Remote-Installation** → **Installationspakete**.

Schritt 6. Konfigurieren von Kaspersky Security Network

Sie können den Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network verwenden, um eine höhere Reaktionsschnelligkeit der Kaspersky-Anwendungen auf Bedrohungen zu gewährleisten, die Effektivität vieler Schutzkomponenten zu erhöhen und die Wahrscheinlichkeit von Fehlalarmen zu verringern.

Lesen Sie die KSN-Erklärung, die im Fenster angezeigt wird. Legen Sie die Einstellungen für die Übertragung von Informationen über die Ausführung von Kaspersky Security Center in die Wissensdatenbank von Kaspersky Security Network fest. Wählen Sie eine der folgenden Varianten aus:

- **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**

  Kaspersky Security Center und die verwalteten Programme, die auf Client-Geräten installiert sind, übertragen ihre Vorgangsdetails automatisch an Kaspersky Security Network. Die Zusammenarbeit mit Kaspersky Security Network gewährleistet ein schnelleres Datenbanken-Update mit Daten über Viren und Bedrohungen, wodurch die Reaktionsgeschwindigkeit auf neue Sicherheitsgefährdungen erhöht wird.

- **Ich stimme der Verwendung von Kaspersky Security Network nicht zu**

  Kaspersky Security Center und verwaltete Programme senden keine Informationen an Kaspersky Security Network.

  Wenn Sie diese Option auswählen, wird die Verwendung von Kaspersky Security Network deaktiviert.

Wenn Sie das Plug-in für Kaspersky Endpoint Security für Windows heruntergeladen haben, werden zwei KSN-Erklärungen angezeigt: Die KSN-Erklärung für Kaspersky Security Center und die KSN-Erklärung für Kaspersky Endpoint Security für Windows. KSN-Erklärungen für andere verwaltete Kaspersky-Anwendungen, deren Plug-ins heruntergeladen wurden, werden in separaten Fenstern angezeigt. Sie müssen jede dieser Erklärungen einzeln akzeptieren (oder ablehnen).

Sie können in der Verwaltungskonsole im Eigenschaftenfenster des Administrationsservers den Zugriff des Administrationsservers auf das Kaspersky Security Network (KSN) auch später einrichten.

Schritt 7. Konfigurieren von E-Mail-Benachrichtigungen

Passen Sie den Versand von Benachrichtigungen über Ereignisse an, die bei der Ausführung von Kaspersky-Anwendungen auf den verwalteten Geräten registriert werden. Diese Einstellungen werden als Standardeinstellungen für den Administrationsserver verwendet.

Folgende Einstellungen für den Versand von Benachrichtigungen über auftretende Ereignisse der Kaspersky-Anwendungen können angepasst werden:

- **Empfänger (E-Mail-Adressen)**

  E-Mail-Adressen des Nutzers, an die das Programm Benachrichtigungen versenden soll. Sie können eine oder mehrere Adressen angeben. Geben Sie mehrere Adressen durch Semikolon getrennt an.

- **SMTP-Server**

  Adresse oder Adressen der Mail-Server Ihres Unternehmens.

Geben Sie mehrere Adressen durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- Windows-Netzwerkname (NetBIOS-Name) des Geräts
- DNS-Name des SMTP-Servers

- **Port des SMTP-Servers**

  Kommunikationsportnummer des SMTP-Servers Wenn Sie mehrere SMTP-Server verwenden, wird die Verbindung zu diesen über den angegebenen Kommunikationsport hergestellt. Standardmäßig wird Portnummer 25 verwendet.

- **ESMTP-Authentifizierung verwenden**

  Aktivierung der Unterstützung von ESMTP-Authentifizierung. Nach der Aktivierung des Kontrollkästchens in den Feldern **Benutzername** und **Kennwort** können die Einstellungen für ESMTP-Authentifizierung angeben werden. Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Einstellungen**

  Geben Sie die folgenden Einstellungen an:

  - **Betreff** (Betreff einer E-Mail-Nachricht)
  - **E-Mail-Adresse des Absenders**
  - **TLS-Einstellungen für SMTP-Server**

  Sie können die TLS-Einstellungen für den SMTP-Server angeben:

  Sie können entweder die Verwendung von TLS deaktivieren, TLS verwenden, wenn der SMTP-Server dieses Protokoll unterstützt, oder die Verwendung von TLS erzwingen. Wenn Sie nur TLS verwenden möchten, geben Sie ein Zertifikat für die Authentifizierung des SMTP-Servers an und wählen Sie aus, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie in dem Fall, dass Sie nur TLS verwenden möchten, ein Zertifikat für die Client-Authentifizierung am SMTP-Server angeben.

  - Geben Sie eine Datei mit SMTP-Server-Zertifikat an:

  Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center prüft, ob das Zertifikat eines SMTP-Servers auch von eine vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

  - Geben Sie die Datei des Client-Zertifikats an:

  Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen Zertifizierungsstelle. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

  - X-509-Zertifikat:

Geben Sie die Datei mit dem Zertifikat und die Datei mit dem privaten Schlüssel an. Sie können diese Dateien in beliebiger Reihenfolge hochladen. Wenn beide Dateien geladen sind, geben Sie das Kennwort zum Entschlüsseln des privaten Schlüssels an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- pkcs12-Container:

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

Sie können die festgelegten Versandeinstellungen der E-Mail-Benachrichtigungen mithilfe der Schaltfläche **Testnachricht senden** prüfen.

Sie können die Ereignisbenachrichtigungen auch später konfigurieren, unabhängig vom Schnellstartassistenten.

Schritt 8. Konfigurieren der Update-Verwaltung

Passen Sie die Einstellungen für die Arbeit mit den Updates der Programme, die auf den Client-Geräten installiert sind, an.

Sie können diese Einstellungen nur konfigurieren, wenn Sie einen Lizenzschlüssel mit der Option "Schwachstellen- und Patch-Management" zur Verfügung angegeben haben.

Im Einstellungsblock **Updates suchen und installieren** können Sie einen der Modus für die Suche und Installation von Updates für Kaspersky Security Center auswählen:

- **Nach erforderlichen Updates suchen**

  Falls die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* noch nicht vorhanden ist, wird sie automatisch erstellt.

  Diese Option ist standardmäßig ausgewählt.

- **Erforderliche Updates suchen und installieren**

  Die Aufgaben *Suche nach Schwachstellen und erforderlichen Updates* und *Erforderliche Updates installieren und Schwachstellen schließen* werden automatisch erstellt, sofern sie noch nicht vorhanden sind.

Im Einstellungsblock **Windows Server Update Services** können Sie die Quelle zur Synchronisierung von Updates auswählen:

- **Verwendung von Update-Quellen, die in der Domänenrichtlinie definiert sind**

  Die Client-Geräte laden Windows-Updates in Übereinstimmung mit den Einstellungen Ihrer Domänenrichtlinie herunter. Die Richtlinie des Administrationsagenten wird automatisch erstellt, sofern sie noch nicht vorhanden ist.

- **Administrationsserver als WSUS-Server verwenden**

  Die Client-Geräte laden Windows-Updates vom Administrationsserver herunter. Die Aufgabe *Windows-Updates synchronisieren* und die Richtlinie des Administrationsagenten werden automatisch erstellt, sofern sie noch nicht vorhanden sind.

Sie können die Aufgaben *Suche nach Schwachstellen und erforderlichen Updates* und *Erforderliche Updates installieren und Schwachstellen schließen* separat vom Schnellstartassistenten erstellen. Um den Administrationsserver als WSUS-Server zu verwenden, erstellen Sie die Aufgabe *Windows-Updates synchronisieren* und wählen Sie anschließend die Option **Administrationsserver als WSUS-Server verwenden** in der Richtlinie des Administrationsagenten.

Schritt 9. Konfigurieren des ersten Schutzes

Im Fenster **Erstkonfiguration des Schutzes anlegen** wird eine Liste der automatisch erstellten Richtlinien und Aufgaben angezeigt. Die folgenden Richtlinien und Aufgaben werden erstellt:

- Die Richtlinie für den Kaspersky Security Center Administrationsagenten
- Richtlinien für verwaltete Kaspersky-Anwendungen, deren Verwaltungs-Plug-Ins zuvor installiert wurden
- Aufgabe Wartung des Administrationsservers
- Aufgabe Backup der Daten des Administrationsservers anlegen
- Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers
- Aufgabe Suche nach Schwachstellen und erforderlichen Updates
- Aufgabe Update installieren

Bevor Sie zum nächsten Schritt des Assistenten wechseln können, müssen Sie warten, bis die Erstellung der Richtlinien und Aufgaben abgeschlossen ist.

Wenn Sie das Plug-in für Kaspersky Endpoint Security für Windows 10 Service Pack 1 und höher (bis Version 11.0.1) heruntergeladen und installiert haben, öffnet sich beim Erstellen von Richtlinien und Aufgaben ein Fenster zur Erstkonfiguration der vertrauenswürdigen Zone von Kaspersky Endpoint Security für Windows. Das Programm schlägt vor, von Kaspersky geprüfte Hersteller zur vertrauenswürdigen Zone hinzuzufügen, damit deren Programme aus der Untersuchung ausgeschlossen und zufällige Blockierungen verhindert werden. Sie können die empfohlenen Ausschlüsse sofort erstellen oder später unter dem folgenden Punkt der Konsolenstruktur eine Liste mit Ausschlüssen anlegen: **Richtlinien** → Eigenschaftenmenü von Kaspersky Endpoint Security → **Erweiterter Schutz** → **Vertrauenswürdige Zone** → **Einstellungen** → **Hinzufügen**. Die Liste der Ausschlüsse aus der Untersuchung kann während der Verwendung des Programms jederzeit bearbeitet werden.

> Die Arbeit mit der vertrauenswürdigen Zone erfolgt mithilfe des Programms Kaspersky Endpoint Security für Windows. Ausführliche Anweisungen zur Ausführung der Vorgänge und eine Beschreibung der Besonderheiten der Verschlüsselungsfunktion können Sie der Online-Hilfe für Kaspersky Endpoint Security für Windows entnehmen.

Um die Erstkonfiguration der vertrauenswürdigen Zone anzuschließen und zum Assistenten zurückzukehren, klicken Sie auf **OK**.

Klicken Sie auf die Schaltfläche **Weiter**. Sie ist verfügbar, wenn alle erforderlichen Richtlinien und Aufgaben erstellt sind.

Sie können die erforderlichen Aufgaben und Richtlinien auch später erstellen, unabhängig vom Schnellstartassistenten.

Schritt 10. Verbinden mobiler Geräte

Wenn Sie in den Einstellungen des Assistenten zuvor den Schutzbereich **Mobile Geräte** aktiviert haben, passen Sie die Verbindungseinstellungen für mobile Unternehmensgeräte des verwalteten Unternehmens an. Wenn Sie den Schutzbereich **Mobile Geräte** nicht aktiviert haben, wird dieser Schritt übersprungen.

Bei diesem Schritt des Assistenten führen Sie die folgenden Aktionen aus:

- Konfigurieren der Ports für die Verbindung mobiler Geräte
- Konfigurieren der Authentifizierung am Administrationsserver
- Erstellen oder verwalten von Zertifikaten
- Anpassen der Ausstellung, der automatischen Aktualisierung und der Verschlüsselung von allgemeinen Zertifikaten
- Erstellen einer Verschiebungsregel für mobile Geräte

Um die Ports für die Verbindung mobiler Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Anpassen** rechts des Feldes **Mobile Geräte verbinden**.
2. Wählen Sie in der Dropdown-Liste die Option **Ports konfigurieren**.

   Das Eigenschaftenfenster des Administrationsservers im Abschnitt **Zusätzliche Ports** wird geöffnet.
3. Im Abschnitt **Zusätzliche Ports** können Sie die Verbindungseinstellungen für mobile Geräte anpassen:

   - **SSL-Port des Aktivierungs-Proxyservers**

     SSL-Portnummer für Verbindung von Kaspersky Endpoint Security für Windows mit den Aktivierungsservern von Kaspersky.

     Standardmäßig wird Portnummer 17000 verwendet.

   - **Port für mobile Geräte öffnen**

     Es wird ein Port für mobile Geräte zur Verbindung mit dem Lizenzserver geöffnet. Sie können die Portnummer und andere Einstellungen in den Feldern weiter unten festlegen.

     Diese Option ist standardmäßig aktiviert.

   - **Port zur Synchronisierung mobiler Geräte**

     Portnummer, über den die mobilen Geräte mit dem Administrationsserver verbunden werden und Informationen mit ihm austauschen. Standardmäßig wird Portnummer 13292 verwendet.

     Sie können einen anderen Port angeben, wenn Port 13292 für andere Zwecke verwendet wird.

   - **Port zur Aktivierung mobiler Geräte**

     Port für die Verbindung von Kaspersky Endpoint Security für Android mit den Aktivierungsservern von Kaspersky.

     Standardmäßig wird Portnummer 17100 verwendet.

- **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS öffnen**

  Geräte mit Schutz auf UEFI-Ebene können eine Verbindung mit dem Administrationsserver herstellen.

- **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS**

  Sie können die Portnummer ändern, wenn die Option **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS öffnen** aktiviert ist. Standardmäßig wird Portnummer 13294 verwendet.

- **Port für Prometheus öffnen**

  Prometheus führt Pull-Requests über diesen Port durch. Standardmäßig wird Portnummer 13296 verwendet.

4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und zum Schnellstartassistenten zurückzukehren.

Sie müssen die Authentifizierung des Administrationsservers durch mobile Geräte sowie die Authentifizierung von mobilen Geräten durch den Administrationsserver anpassen. Wenn gewünscht, können Sie die Authentifizierung auch zu einem späteren Zeitpunkt außerhalb des Schnellstartassistenten konfigurieren.

Um die Authentifizierungseinstellungen des Administrationsservers für die mobilen Geräte anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Anpassen** rechts des Feldes **Mobile Geräte verbinden**.

2. Wählen Sie in der Dropdown-Liste die Option **Authentifizierung konfigurieren**.

   Das Eigenschaftenfenster des Administrationsservers im Abschnitt **Zertifikate** wird geöffnet.

3. Wählen Sie die Authentifizierungsoption für mobile Geräte in der Einstellungsgruppe **Authentifizierung des Administrationsservers durch mobile Geräte** aus, und wählen Sie die Authentifizierungsoption für UEFI-Schutzgeräte in der Einstellungsgruppe **Authentifizierung des Administrationsservers durch Geräte mit Schutz auf UEFI-Ebene** aus.

   Die Authentifizierung des Administrationsservers beim Datenaustausch mit den Client-Geräten erfolgt mithilfe des Zertifikats.

   Standardmäßig ist die Variante zur Nutzung jenes Zertifikats ausgewählt, das bei der Installation des Administrationsservers erstellt wurde. Bei Bedarf können Sie ein neues Zertifikat hinzufügen.

Um ein neues Zertifikat hinzuzufügen, gehen Sie wie folgt vor (optional):

1. Wählen Sie **Anderes Zertifikat** aus.

   Die Schaltfläche **Durchsuchen** wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Durchsuchen**.

3. Passen Sie im nächsten Fenster die Einstellungen des Zertifikats an:

   - **Zertifikatstyp**

     In dieser Dropdown-Liste können Sie einen Zertifikatstyp auswählen:

     - **X.509-Zertifikat**. Wenn diese Option ausgewählt ist, müssen Sie den privaten Schlüssel des Zertifikats

sowie ein offenes Zertifikat angeben:

- **Privater Schlüssel (.prk, .pem)**. Klicken Sie in diesem Feld auf **Durchsuchen**, um den privaten Schlüssel des Zertifikats im Format PKCS #8 (*.prk) anzugeben.
- **Offener Schlüssel (.cer)**. Klicken Sie in diesem Feld auf **Durchsuchen**, um einen öffentlichen Schlüssel im Format PEM (*.cer) anzugeben.

- **Container PKCS#12**. Wenn Sie diese Option auswählen, können Sie eine Zertifikatsdatei im Format P12 oder PFX angeben, indem Sie auf **Durchsuchen** klicken und das Feld **Zertifikatdatei** ausfüllen.

- Aktivierungsfrist:
  - **Sofort**

    Das aktuelle Zertifikat wird sofort nach dem Klick auf **OK** durch das neue Zertifikat ersetzt.

    Früher verbundene mobile Geräte können keine Verbindung zum Administrationsserver herstellen.

  - **Innerhalb der angegebenen Frist (Tage)**

    Wenn diese Variante ausgewählt ist, so wird ein Reserve-Zertifikat generiert. Das aktuelle Zertifikat wird nach der angegebenen Anzahl von Tagen durch das neue Zertifikat ersetzt. Das Datum, an dem das Reserve-Zertifikat in Kraft tritt, wird im Abschnitt **Zertifikate** angezeigt.

    Es wird empfohlen, die Neuausstellung im Voraus zu planen. Das Reserve-Zertifikat muss vor Ablauf des angegebenen Zeitraums auf die mobilen Geräte heruntergeladen werden. Nachdem das aktuelle Zertifikat durch das neue Zertifikat ersetzt wurde, können früher verbundene mobile Geräte, die über kein Reserve-Zertifikat verfügen, keine Verbindung mit dem Administrationsserver herstellen.

4. Mithilfe der Schaltfläche **Eigenschaften** können Sie die Einstellungen des ausgewählten Zertifikats des Administrationsservers anzeigen.

Um ein Zertifikat, das mithilfe des Administrationsservers ausgestellt wurde, neu auszustellen:

1. Wählen Sie **Das Zertifikat wurde mithilfe des Administrationsservers ausgestellt** aus.
2. Klicken Sie auf die Schaltfläche **Neu ausstellen**.
3. Passen Sie im nächsten Fenster folgende Einstellungen an:
   - Adresse der Verbindung:
     - **Vorherige Verbindungsadresse beibehalten**

       Die Adresse des Administrationsservers, mit der die mobilen Geräte verbunden werden, bleibt unverändert.

       Diese Variante ist standardmäßig festgelegt.

     - **Verbindungsadresse ändern auf**

       Wenn mobile Geräte über eine andere Adresse verbunden werden sollen, geben Sie im Feld die erforderliche Adresse an.

       Bei einer Änderung der Adresse für die Verbindung von mobilen Geräten muss ein neues Zertifikat ausgestellt werden. Das alte Zertifikat wird auf den verbundenen mobilen Geräten ungültig. Früher verbundene Geräte können keine Verbindung zum Administrationsserver herstellen und werden nicht mehr verwaltet.

- Aktivierungsfrist:

  - **Sofort**

    Das aktuelle Zertifikat wird sofort nach dem Klick auf **OK** durch das neue Zertifikat ersetzt.

    Früher verbundene mobile Geräte können keine Verbindung zum Administrationsserver herstellen.

  - **Innerhalb der angegebenen Frist (Tage)**

    Wenn diese Variante ausgewählt ist, so wird ein Reserve-Zertifikat generiert. Das aktuelle Zertifikat wird nach der angegebenen Anzahl von Tagen durch das neue Zertifikat ersetzt. Das Datum, an dem das Reserve-Zertifikat in Kraft tritt, wird im Abschnitt **Zertifikate** angezeigt.

    Es wird empfohlen, die Neuausstellung im Voraus zu planen. Das Reserve-Zertifikat muss vor Ablauf des angegebenen Zeitraums auf die mobilen Geräte heruntergeladen werden. Nachdem das aktuelle Zertifikat durch das neue Zertifikat ersetzt wurde, können früher verbundene mobile Geräte, die über kein Reserve-Zertifikat verfügen, keine Verbindung mit dem Administrationsserver herstellen.

4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und zum Fenster **Zertifikate** zurückzukehren.

5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und zum Schnellstartassistenten zurückzukehren.

Um die Ausstellung, das automatische Update und die Verschlüsselung der allgemeinen Zertifikate für die Identifizierung von mobilen Geräten durch den Administrationsserver anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Anpassen** rechts im Feld **Authentifizierung mobiler Geräte**.

   Das Fenster **Regeln für das Ausstellen von Zertifikaten** wird geöffnet. Darin wird der Abschnitt **Mobilgerät-Zertifikat ausstellen** angezeigt.

2. Legen Sie erforderlichenfalls die folgenden Einstellungen im Einstellungsblock **Ausstellungseinstellungen** fest:

   - **Gültigkeitsdauer des Zertifikats, Tage**

     Gültigkeitsdauer des Zertifikats in Tagen. Standardmäßig beträgt die Gültigkeitsdauer des Zertifikats 365 Tage. Nach Ablauf dieses Zeitraums kann das mobile Gerät keine Verbindung mit dem Administrationsserver mehr herstellen.

   - **Quelle des Zertifikats**

     Auswahl der Quelle eines allgemeinen Zertifikats für mobile Geräte: die Zertifikate werden vom Administrationsserver ausgestellt oder die Zertifikate werden manuell erstellt.

     Sie können die Zertifikatsvorlage anpassen, wenn im Abschnitt **PKI-Integration** die Integration mit Public-Key-Infrastruktur (PKI) ausgewählt ist. In diesem Fall sind die folgenden Felder zur Auswahl der Vorlage verfügbar:

   - **Standardvorlage**

     Nutzung des Zertifikates, das von der externen Quelle der Zertifikate, dem Zentrum der Zertifizierung, ausgegeben wurde, gemäß der standardmäßig festgelegten Vorlage.

     Diese Variante ist standardmäßig ausgewählt.

- **Andere Vorlage**

  Auswahl der Vorlage, auf deren Grundlage die Zertifikate ausgestellt werden. Zertifikatsvorlagen können in der Domäne angegeben werden. Mithilfe der Schaltfläche **Liste aktualisieren** können Sie die Liste der Zertifikatsvorlagen aktualisieren.

3. Legen Sie erforderlichenfalls die folgenden Einstellungen für die automatische Ausgabe der Zertifikate im Einstellungsblock **Einstellungen für das automatische Update** fest:

   - **Erneuerung bevor das Zertifikat abläuft in (Tagen)**

     Anzahl der Tage bis zum Ablauf der Gültigkeitsdauer des aktuellen Zertifikats, während der vom Administrationsserver ein neues Zertifikat ausgestellt werden muss. Wenn in diesem Feld beispielsweise der Wert 4 angegeben ist, stellt der Administrationsserver innerhalb von vier Tagen vor Ablauf der Gültigkeitsdauer des aktuellen Zertifikats ein neues Zertifikat aus. Als Standardwert ist 7 vorgegeben.

   - **Zertifikat automatisch neu veröffentlichen, falls möglich**

     Wählen Sie diese Option, um ein Zertifikat automatisch für die in dem Feld **Erneuerung bevor das Zertifikat abläuft in (Tagen)** angegebene Anzahl von Tagen neu auszustellen. Wenn ein Zertifikat manuell angegeben wurde, kann es nicht automatisch verlängert werden und die aktivierte Option bleibt ohne Funktion.

     Diese Option ist standardmäßig deaktiviert.

   Die Zertifikate werden durch eine Zertifizierungsstelle automatisch neu ausgestellt.

4. Legen Sie die Einstellungen für die Entschlüsselung der Zertifikate bei der Installation erforderlichenfalls im Einstellungsblock **Kennwortschutz** fest.

   Aktivieren Sie die Option **Bei der Installation des Zertifikats Kennwort abfragen**, damit bei der Installation des Zertifikates auf dem mobilen Gerät vom Benutzer das Kennwort abgefragt wird. Das Kennwort wird nur einmal bei der Installation des Zertifikats auf dem mobilen Gerät verwendet.

   Das Kennwort wird automatisch mithilfe des Administrationsservers generiert und an die von Ihnen angegebene E-Mail-Adresse gesendet. Sie können die E-Mail-Adresse eines Benutzers oder eine eigene Adresse angeben, wenn Sie dem Benutzer das Kennwort auf andere Weise übermitteln möchten.

   Sie können mithilfe der Schiebereglers die Anzahl der Zeichen des Kennworts für die Entschlüsselung des Zertifikates festlegen.

   Die Funktion der Kennwortabfrage ist beispielsweise für den Schutz des allgemeinen Zertifikates im autonomen Installationspaket von Kaspersky Endpoint Security für Android erforderlich. Der Kennwortschutz verhindert, dass ein Angreifer bei einem Diebstahl des autonomen Installationspakets des Kaspersky Security Center Webservers Zugriff auf das allgemeine Zertifikat erhält.

   Wenn die Option deaktiviert ist, wird die Entschlüsselung des Zertifikats bei der Installation automatisch durchgeführt und der Benutzer wird nicht nach dem Kennwort gefragt. Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und zum Schnellstartassistenten zurückzukehren.

   Klicken Sie auf die Schaltfläche **Abbrechen**, um zum Schnellstartassistenten zurückzukehren, ohne die Änderungen zu speichern.

Um die Funktion zum Verschieben der mobilen Geräte in die gewünschte Administrationsgruppe zu aktivieren,

Wählen Sie im Feld **Automatisches Verschieben mobiler Geräte** die Option **Verschiebungsregel für mobile Geräte erstellen**.

Wenn die Option **Verschiebungsregel für mobile Geräte erstellen** aktiviert ist, erstellt das Programm automatisch eine Verschiebungsregel, die folgende Android- und iOS-Geräte in die Gruppe **Verwaltete Geräte** verschiebt:

- Geräte mit Android-Betriebssystemen, auf denen Kaspersky Endpoint Security für Android und ein Mobilgerät-Zertifikat installiert sind
- Geräte mit iOS-Betriebssystemen, auf denen das iOS MDM-Profil mit einem freigegebenen Zertifikat installiert ist

Wenn eine solche Regel schon existiert, wird keine Regel erstellt.

Diese Option ist standardmäßig deaktiviert.

Kaspersky stellt die Unterstützung für Kaspersky Safe Browser ein.

Schritt 11. Herunterladen von Updates

Updates für die Antiviren-Datenbanken von Kaspersky Security Center und für verwaltete Kaspersky-Anwendungen werden automatisch heruntergeladen. Die Updates werden automatisch von Kaspersky-Servern heruntergeladen.

Um Updates unabhängig vom Schnellstartassistenten herunterzuladen, erstellen und konfigurieren Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers anpassen*.

Schritt 12. Suchen von Geräten

Im Informationsfenster **Netzwerkabfrage** werden Informationen über den Status der Netzwerkabfrage des Administrationsservers angezeigt.

Sie können im Netzwerk vom Administrationsserver erkannte Geräte anzeigen und erhalten mithilfe der Links im unteren Bereich des Fensters Hilfe zur Arbeit mit dem Fenster **Gerätesuche**.

Sie können Ihr Netzwerk später, unabhängig vom Schnellstartassistenten, abfragen. Verwenden Sie die Verwaltungskonsole, um die Abfrage der Windows-Domänen, des Active Directory, der IP-Bereiche und der IPv6-Netzwerke zu konfigurieren.

Schritt 13. Abschließen des Schnellstartassistenten

Aktivieren Sie im Fenster "Schnellstartassistent abschließen" die Option **Assistent für Remote-Installationen starten**, wenn Sie die automatische Installation der Antiviren-Programme und/oder des Administrationsagenten auf den Geräten in Ihrem Netzwerk starten möchten.

Klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.

Verbindung der Verwaltungskonsole mit dem Administrationsserver anpassen

Die Verwaltungskonsole ist über den SSL-Port TCP 13291 mit dem Administrationsserver verbunden. Derselbe Port kann von klakaut-Automatisierungsobjekten verwendet werden.

Der Port TCP 14000 kann für die Verbindung der Verwaltungskonsole, der Verteilungspunkte, der sekundären Administrationsserver und der Automatisierungsobjekte des Tools klakaut sowie für das Abrufen der Daten von den Client-Geräten verwendet werden.

Der SSL-Port TCP 13000 kann normalerweise nur vom Administrationsagenten, einem sekundären Administrationsserver und dem primären Administrationsserver in der DMZ verwendet werden. In einigen Fällen kann eine Verbindung der Verwaltungskonsole über den SSL-Port 13000 erforderlich sein:

- Bei Verwendung desselben SSL-Ports sowohl für die Verwaltungskonsole als auch für andere Aktivitäten (Abrufen der Daten von den Client-Geräten, Verbindung mit Verteilungspunkten, Verbindung mit sekundären Administrationsservern).

- Wenn das Automatisierungsobjekt des Tools klakaut nicht direkt mit dem Administrationsserver, sondern über den Verteilungspunkt in der DMZ verbunden wird.

Um eine Verbindung der Verwaltungskonsole über den Port 13000 zu erlauben, gehen Sie wie folgt vor:

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsserver installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** > **Ausführen**.

2. Rufen Sie den folgenden Abschnitt auf:

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM.

   - Für 64-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Für den Schlüssel LP_ConsoleMustUsePort13291 (DWORD) ist der Wert 00000000 festgelegt.

   Standardmäßig wird für diesen Schlüssel der Wert 1 festgelegt.

4. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin kann die Verwaltungskonsole mit dem Administrationsserver über den Port 13000 eine Verbindung herstellen.

Die Internetzugriffseinstellungen für den Administrationsserver konfigurieren

Sie müssen den Internetzugang anpassen, um Kaspersky Security Network zu verwenden und um Updates für die Antiviren-Datenbanken von Kaspersky Security Center und die verwalteten Kaspersky-Anwendungen herunterzuladen.

So geben Sie die Internetzugriffseinstellungen für den Administrationsserver an:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver** aus.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wechseln Sie im Eigenschaftenfenster des Administrationsservers zu **Erweitert → Einstellungen für den Internetzugriff konfigurieren**.
4. Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

   - **Adresse**

     Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center mit dem Internet.

   - **Port**

     Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center hergestellt wird.

   - **Proxyserver für lokale Adressen umgehen**

     Bei der Verbindung mit den Geräten im lokalen Netzwerk wird kein Proxyserver verwendet.

   - **Authentifizierung am Proxyserver**

     Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

     Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver verwenden** aktiviert ist.

   - **Benutzername**

     Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

   - **Kennwort**

     Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

     Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

Sie können den Internetzugang auch unter Verwendung des Schnellstartassistenten konfigurieren.

Verbinden mobiler Geräte

Dieser Abschnitt beschreibt, wie Sie mobile Geräte (d.h. verwaltete Geräte, die sich außerhalb des Hauptnetzwerks befinden) mit dem Administrationsserver verbinden.

Szenario: Verbinden von mobilen Geräten mittels Verbindungs-Gateway

Dieses Szenario beschreibt, wie Sie verwaltete Geräte, die sich außerhalb des Hauptnetzwerks befinden, mit dem Administrationsserver verbinden.

Erforderliche Vorrausetzungen

Für dieses Szenario müssen die folgenden Voraussetzungen erfüllt sein:

- Eine demilitarisierte Zone (DMZ) ist im Netzwerk Ihrer Organisation eingerichtet.
- Ein Kaspersky Security Center Administrationsserver ist im Unternehmensnetzwerk bereitgestellt.

Schritte

Das Szenario verläuft in Stufen:

1. **Auswählen eines Client-Gerätes innerhalb der DMZ**

   Das Gerät wird als Verbindungs-Gateway verwendet. Das von Ihnen ausgewählte Gerät muss den Anforderungen an ein Verbindungs-Gateway entsprechen.

2. **Installation des Administrationsagenten für seine Rolle als Verbindungs-Gateway**

   Für die Installation des Administrationsagenten auf dem ausgewählten Gerät wird eine lokale Installation empfohlen.

   Standardmäßig befindet sich die Installationsdatei unter: \\<Servername>\KLSHARE\PkgInst\NetAgent_<Versionsnummer>

   Wählen Sie im Installationsassistenten des Administrationsagenten im Fenster **Verbindungs-Gateway** die Option **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden**. Dieser Modus aktiviert die Rolle als Verbindungs-Gateway und unterweist gleichzeitig den Administrationsagenten, auf Verbindungen vom Administrationsserver zu warten, anstelle Verbindungen zum Administrationsserver herzustellen.

   Alternativ können Sie den Administrationsagent auf einem Linux-Gerät installieren und so konfigurieren, dass er als Verbindungs-Gateway fungiert, sollten dabei aber die Liste der Einschränkungen von Administrationsagenten auf Linux-Geräten beachten.

3. **Erlauben von Verbindungen in den Firewalls auf dem Verbindungs-Gateway**

   Um sicherzustellen, dass sich der Administrationsserver tatsächlich mit dem Verbindungs-Gateway in der DMZ verbinden kann, erlauben Sie Verbindungen zu TCP-Port 13000 in allen Firewalls zwischen dem Administrationsserver und dem Verbindungsgateway.

   Wenn das Verbindungs-Gateway keine echte IP-Adresse im Internet besitzt, sich aber stattdessen hinter einer Network Address Translation (NAT) befindet, konfigurieren Sie eine Regel für das Forwarding von Verbindungen über NAT.

4. **Erstellen einer Administrationsgruppe für externe Geräte**

   Erstellen Sie eine neue Gruppe unter der Gruppe **Managed devices**. Diese neue Gruppe wird die externen verwalteten Geräte enthalten.

5. **Verbinden des Verbindungs-Gateways mit dem Administrationsserver**

Das von Ihnen konfigurierte Verbindungs-Gateway wartet auf eine Verbindung vom Administrationsserver. Der Administrationsserver zeigt das Gerät mit dem Verbindungs-Gateway jedoch nicht unter den verwalteten Geräten an. Das liegt daran, dass das Verbindungs-Gateway noch nicht versucht hat, eine Verbindung mit dem Administrationsserver herzustellen. Es ist daher eine spezielle Vorgehensweise notwendig, um sicherzustellen, dass der Administrationsserver eine Verbindung zum Verbindungs-Gateway initiiert.

Führen Sie folgende Schritte aus:

1. Fügen Sie das Verbindungs-Gateway als Verteilungspunkt hinzu.
2. Verschieben Sie das Verbindungs-Gateway von der Gruppe **Nicht zugeordnete Geräte** in die Gruppe, die Sie für externe Geräte angelegt haben.

Das Verbindungs-Gateway ist verbunden und konfiguriert.

6 Verbinden von externen Desktop-Geräten mit dem Administrationsserver

In der Regel werden externe Desktop-Geräte nicht in den Perimeter hinein bewegt. Daher müssen Sie die Geräte während der Installation des Administrationsagenten so konfigurieren, dass sie sich über das Verbindungs-Gateway mit dem Administrationsserver verbinden.

7 Konfigurieren von Updates für externe Desktop-Geräte

Wenn die Updates der Sicherheitsanwendungen so konfiguriert sind, dass sie vom Administrationsserver heruntergeladen werden, laden sich externe Geräte die Updates über das Verbindungs-Gateway herunter. Das hat zwei Nachteile:

- Es entsteht unnötiger Traffic, welcher Bandbreite vom Internet-Kommunikationskanal des Unternehmens in Beschlag nimmt.
- Es ist nicht zwangsläufig die schnellste Art, Updates zu beziehen. Es ist anzunehmen, dass es für externe Geräte günstiger und schneller wäre, ihre Updates von Kaspersky-Update-Servern zu beziehen.

Führen Sie folgende Schritte aus:

1. Verschieben Sie alle externen Geräte in die separate Administrationsgruppe, die Sie zu einem früheren Zeitpunkt angelegt haben.
2. Schließen Sie die Gruppe mit den externen Geräten von der Update-Aufgabe aus.
3. Erstellen Sie eine separate Update-Aufgabe für die Gruppe mit den externen Geräten.

8 Verbinden von Laptops, die Reisetätigkeiten unterliegen, mit dem Administrationsserver

Reiselaptops befinden sich manchmal innerhalb und manchmal außerhalb des Netzwerks. Um deren Verwaltung effizient zu gestalten, müssen sich diese Geräte, abhängig von deren Standort, auf unterschiedliche Weise mit dem Administrationsserver verbinden. Für effizienten Traffic müssen die Geräte ebenfalls in Abhängigkeit von ihrem Standort Updates aus verschiedenen Quellen beziehen.

Sie müssen Regeln für mobile Benutzer konfigurieren: Verbindungsprofile und Beschreibungen der Standorte im Netzwerk. Jede Regel gibt an, mit welcher Instanz eines Administrationsservers sich die Reiselaptops in Abhängigkeit ihres Standortes verbinden müssen und von welcher Instanz eines Administrationsservers sie ihre Updates beziehen müssen.

Szenario: Verbinden von mobilen Geräten mittels einem sekundären Administrationsserver in der DMZ

Wenn Sie mit dem Administrationsserver verwaltete Geräte verbinden möchten, die sich außerhalb des Hauptnetzwerks befinden, können Sie einen sekundären Administrationsserver verwenden, der sich in der demilitarisierten Zone (DMZ) befindet.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

- Im Netzwerk Ihrer Organisation ist eine DMZ eingerichtet.
- Kaspersky Security Center Administrationsserver wurde im internen Unternehmensnetzwerk bereitgestellt.

Schritte

Das Szenario verläuft in Stufen:

1. **Auswählen eines Client-Gerätes innerhalb der DMZ**

   Wählen Sie in der DMZ ein Client-Gerät aus, das als sekundärer Administrationsserver verwendet werden soll.

2. **Kaspersky Security Center Administrationsserver installieren**

   Installation von Kaspersky Security Center Administrationsserver auf diesem Client-Gerät.

3. **Eine Administrationsserver-Hierarchie erstellen**

   Wenn Sie einen sekundären Administrationsserver in der DMZ platzieren, muss der sekundäre Administrationsserver eine Verbindung vom primären Administrationsserver annehmen können. Fügen Sie dafür einen neuen Administrationsserver als sekundär hinzu, damit sich der primäre Administrationsserver über Port 13000 mit dem sekundären Administrationsserver verbindet. Bei der Zusammenfassung der Administrationsserver in der Hierarchie ist es erforderlich, dass der Port 13291 beider Server verfügbar ist. Die Verwaltungskonsole verbindet sich mit Administrationsserver über Port 13291.

4. **Verwaltete mobile Geräte mit dem sekundären Administrationsserver verbinden**

   Sie können mobile Geräte auf die gleiche Weise mit dem Administrationsserver in der DMZ verbinden, wie beim Verbindungsaufbau zwischen dem Administrationsserver und den verwalteten Geräten, die sich im Hauptnetzwerk befinden. Verwaltete mobile Geräten initiieren die Verbindung über Port 13000.

Über das Verbinden mobiler Geräte

Einige verwaltete Geräte befinden sich dauerhaft außerhalb des Hauptnetzwerks (z. B. Geräte in regionalen Unternehmensniederlassungen, Kiosks, Geldautomaten, an verschiedenen Point-of-Sales installierte Terminals, Geräte im Home-Office von Angestellten). Einige Geräte bewegen sich von Zeit zu Zeit außerhalb des Perimeters (z. B. Laptops von Benutzern, die regionale Niederlassungen oder das Büro eines Kunden besuchen).

Auch von solchen mobilen Geräten muss der Schutz überwacht und verwaltet werden, d. h. es muss möglich sein, aktuelle Informationen über den Schutzstatus der Geräte abzurufen und die auf ihnen installierten Sicherheitsanwendungen aktuell zu halten. Dies ist beispielsweise wichtig für den Fall, in dem ein solches Gerät kompromittiert wird, während es sich außerhalb des Hauptnetzwerks befindet. In der Folge kann das Gerät beim erneuten Verbinden mit dem Hauptnetzwerk zu einer Plattform sich ausbreitender Bedrohungen werden. Sie können zwei Methoden verwenden, um mobile Geräte mit dem Administrationsserver zu verbinden:

- Verbindungs-Gateway in der demilitarisierten Zone (DMZ)

  Schema des Datenverkehrs: Administrationsserver im LAN, verwaltete Geräte im Internet, Verbindungs-Gateway wird verwendet.

- Administrationsserver in der DMZ

  Schema des Datenverkehrs: Administrationsserver in DMZ, verwaltete Geräte im Internet

Ein Verbindungs-Gateway in der DMZ

Eine empfohlene Methode zum Verbinden von mobilen Geräten mit dem Administrationsserver besteht darin, eine DMZ im Netzwerk des Unternehmens zu organisieren und ein Verbindung-Gateway in der DMZ zu installieren. Externe Geräte verbinden sich mit dem Verbindungs-Gateway und der Administrationsserver innerhalb des Netzwerks initiiert die Verbindung zu den Geräten über das Verbindungs-Gateway.

Im Vergleich zu der anderen Methode ist diese sicherer:

- Sie müssen den Zugriff auf den Administrationsserver nicht von außerhalb des Netzwerks öffnen.
- Ein kompromittiertes Verbindungs-Gateway stellt kein hohes Risiko für die Sicherheit der Netzwerkgeräte dar. Ein Verbindungs-Gateway verwaltet im Grunde nichts selbst und stellt keine Verbindungen her.

Außerdem erfordert ein Verbindungs-Gateway nicht viele Hardware-Ressourcen.

Der Konfigurationsprozess dieser Methode ist jedoch komplexer:

- Damit ein Gerät als Verbindungs-Gateway in der DMZ fungiert, müssen Sie den Administrationsagenten installieren und auf eine bestimmte Weise mit dem Administrationsserver verbinden.
- Sie können nicht in allen Situationen dieselbe Adresse für die Verbindung zum Administrationsserver verwenden. Von außerhalb des Perimeters müssen Sie nicht nur eine andere Adresse verwenden (Adresse des Verbindungs-Gateways), sondern auch einen anderen Verbindungsmodus (über ein Verbindungs-Gateway).
- Sie müssen auch unterschiedliche Verbindungseinstellungen für Laptops an verschiedenen Standorten festlegen.

So fügen Sie einem zuvor konfigurierten Netzwerk ein Verbindungs-Gateway hinzu:

1. Installieren Sie Administrationsagenten Verbindungs-Gateway-Modus.
2. Installieren Sie den Administrationsagenten auf den Geräten erneut, die Sie mit dem neu hinzugefügten Verbindungs-Gateway verbinden möchten.

Administrationsserver in der DMZ

Eine andere Methode ist die Installation eines einzelnen Administrationsservers in der DMZ.

Diese Konfiguration ist weniger sicher als die andere Methode. Um in diesem Fall externe Laptops zu verwalten, muss der Administrationsserver Verbindungen von jeder Adresse im Internet akzeptieren. Es werden weiterhin alle Geräte im internen Netzwerk verwaltet, jedoch erfolgt dies aus der DMZ. Daher kann ein kompromittierter Server trotz der geringen Wahrscheinlichkeit eines solchen Ereignisses einen enormen Schaden verursachen.

Das Risiko wird erheblich geringer, wenn der Administrationsserver in der DMZ keine Geräte im internen Netzwerk verwaltet. Eine solche Konfiguration kann beispielsweise von einem Dienstanbieter verwendet werden, um die Geräte von Kunden zu verwalten.

Möglicherweise möchten Sie diese Methode in den folgenden Fällen verwenden:

- Wenn Sie mit der Installation und Konfiguration des Administrationsservers vertraut sind und kein anderes Verfahren zum Installieren und Konfigurieren eines Verbindungsgateways ausführen möchten.
- Wenn Sie mehr Geräte verwalten müssen. Die maximale Kapazität der Administrationsserver beträgt 100.000 Geräte, während ein Verbindungs-Gateway bis zu 10.000 Geräte unterstützen kann.

Auch diese Lösung birgt mögliche Schwierigkeiten:

- Der Administrationsserver benötigt mehr Hardware-Ressourcen und eine zusätzliche Datenbank.
- Informationen zu Geräten werden in zwei unabhängigen Datenbanken gespeichert (für Administrationsserver im Netzwerk und eine weitere in der DMZ), was die Überwachung erschwert.
- Um alle Geräte zu verwalten, muss der Administrationsserver zu einer Hierarchie zusammengefügt werden, was nicht nur die Überwachung, sondern auch die Verwaltung erschwert. Eine Instanz eines sekundären Administrationsservers schränkt die möglichen Strukturen von Administrationsgruppen ein. Sie müssen entscheiden, wie und welche Aufgaben und Richtlinien an eine Instanz eines sekundären Administrationsservers verteilt werden sollen.
- Das Konfigurieren externer Geräte zur Verwendung des Administrationsservers in der DMZ von außen und zur Verwendung des primären Administrationsservers von innen ist komplexer, als sie nur für die Verwendung einer bedingten Verbindung über ein Gateway zu konfigurieren.
- Hohe Sicherheitsrisiken. Eine kompromittierte Instanz eines Administrationsservers erleichtert die Kompromittierung der von ihr verwalteten Laptops. In diesem Fall müssen die Hacker nur warten, bis einer der Laptops zum Unternehmensnetzwerk zurückkehrt, damit sie ihren Angriff auf das lokale Netzwerk fortsetzen können.

Verbinden von externen Desktop-Geräten mit dem Administrationsserver

Geräte, die sich dauerhaft außerhalb des Hauptnetzwerks befinden (z. B. Geräte in regionalen Unternehmensniederlassungen, Kiosks, Geldautomaten, an verschiedenen Point-of-Sales installierte Terminals, Geräte im Home-Office von Angestellten) können nicht direkt mit dem Administrationsserver verbunden werden. Stattdessen müssen sie mit dem Administrationsserver über einen Verbindungs-Gateway verbunden werden, welches in der demilitarisierten Zone (DMZ) platziert ist. Die dafür notwendige Konfiguration wird vorgenommen, wenn der Administrationsagent auf diesen Geräten installiert wird.

Um externe Desktop-Geräte mit dem Administrationsserver zu verbinden:

1. Erstellen ein neues Installationspaket für den Administrationsagenten.
2. Öffnen Sie die Eigenschaften des Installationspakets, wechseln Sie zum Abschnitt **Erweitert** und aktivieren Sie anschließend die Option **Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen**.

   Die Einstellung **Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen** ist inkompatibel zur Einstellung **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden**. Beide Einstellungen können nicht gleichzeitig aktiv sein.

3. Geben Sie in **Verbindungs-Gateway-Adresse** die öffentliche Adresse des Verbindungs-Gateways an.

   Wenn sich der Verbindungs-Gateway hinter einer Network Address Translation (NAT) befindet und keine eigene öffentliche Adresse besitzt, konfigurieren Sie eine NAT-Gateway-Regel für das Forwarding von Verbindungen aus öffentlichen Adressen zur internen Adresse des Verbindungs-Gateways.

4. Erstellen Sie ein autonomes Installationspaket auf Grundlage des erstellten Installationspakets.
5. Übermitteln Sie das autonome Installationspaket entweder elektronisch oder mithilfe eines Wechseldatenträgers an das Zielgerät.
6. Installieren Sie den Administrationsagenten aus dem autonomes Paket.

Die externen Geräte sind mit dem Administrationsserver verbunden.

Über Verbindungsprofile für mobile Benutzer

Bei der Arbeit der mobilen Benutzer, die Laptops (im Weiteren auch "Geräte") verwenden, kann es erforderlich sein, die Verbindungsmethode mit dem Administrationsserver zu ändern oder abhängig von aktuellen Standort des Geräts im Netzwerk zwischen Administrationsservern umzuschalten.

Verbindungsprofile werden nur für Geräte mir Windows oder macOS unterstützt.

Nutzung verschiedener Adressen ein- und desselben Administrationsservers

Die Geräte mit installiertem Administrationsagenten können in unterschiedlichen Zeiträumen sowohl aus dem internen Netzwerk des Unternehmens als auch aus dem Internet mit dem Administrationsserver verbunden werden. In dieser Situation kann es erforderlich sein, dass der Administrationsagent verschiedene Adressen für die Verbindung mit dem Administrationsserver verwendet: die externe Adresse des Servers bei der Verbindung aus dem Internet und die interne Adresse des Servers bei der Verbindung aus dem internen Netzwerk.

Dazu müssen Sie ein Profil (zur Verbindung mit dem Administrationsserver aus dem Internet) zur Richtlinie des Administrationsagenten hinzufügen. Fügen Sie das Profil in den Richtlinieneigenschaften (Abschnitt **Konnektivität**, Unterabschnitt **Verbindungsprofile**) hinzu. Deaktivieren Sie im Fenster für die Profilerstellung die Option **Nur für Update-Download verwenden** und aktivieren Sie die Option **Verbindungseinstellungen mit den Einstellungen für den Administrationsserver synchronisieren, die in diesem Profil angegeben sind**. Wenn für den Zugriff auf den Administrationsserver ein Verbindungs-Gateway verwendet wird (beispielsweise in einer Konfiguration von Kaspersky Security Center vom Typ Zugriff aus dem Internet: Administrationsagent als Verbindungs-Gateway in der demilitarisierten Zone), muss im Verbindungsprofil die Adresse des Verbindungs-Gateways im entsprechenden Feld angegeben werden.

Umschaltung zwischen Administrationsservern in Abhängigkeit vom aktuellen Netzwerk

Wenn es im Unternehmen mehrere Büros mit verschiedenen Administrationsservern gibt und zwischen ihnen ein Teil der Geräte mit installiertem Administrationsagenten verschoben wird, ist es erforderlich, dass der Administrationsagent mit dem Administrationsserver des lokalen Netzwerkes jenes Büros verbunden wird, in dem sich das Gerät befindet.

In diesem Fall ist es erforderlich, in den Eigenschaften der Richtlinie des Administrationsagenten das Profil für Verbindung mit Administrationsserver für jedes der Büros mit Ausnahme des Büros zu erstellen, in dem sich der Home-Administrationsserver befindet. In den Verbindungsprofilen müssen die Adressen der entsprechenden Administrationsserver angegeben werden und die Option **Nur für Update-Download verwenden** entweder aktiviert oder deaktiviert werden:

- Aktivieren Sie die Option, wenn es erforderlich ist, dass sich der Administrationsagent mit dem Home-Administrationsserver synchronisiert und der lokale Server nur für den Update-Download verwendet wird.
- Deaktivieren Sie diese Option, wenn erforderlich ist, dass der Administrationsagent den lokalen Administrationsserver vollständig verwaltet.

Des Weiteren müssen die Bedingungen für die Umschaltung auf die erstellten Profile angepasst werden: mindestens eine Bedingung für jedes Büro, mit Ausnahme des "Home-Office". Der Sinn jeder solchen Bedingung besteht in der Sichtbarkeit der büroeigenen Details in der Netzwerkumgebung. Wenn eine Bedingung erfüllt wird, erfolgt die Aktivierung des entsprechenden Profils. Trifft keine der Bedingungen zu, wird der Administrationsagent auf den Home-Administrationsserver umgeschaltet.

Erstellen eines Verbindungsprofils für mobile Benutzer

Ein Profil zur Verbindung mit dem Administrationsserver steht nur auf Geräten mit Windows oder macOS zur Verfügung.

Um für mobile Benutzer ein Profil für die Verbindung des Administrationsagenten zum Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe, für deren Client-Geräte ein Profil für die Verbindung des Administrationsagenten zum Administrationsserver erstellt werden soll.

2. Führen Sie eine der folgenden Aktionen aus:

   - Um ein Verbindungsprofil für alle Geräte der Gruppe zu erstellen, wählen Sie im Arbeitsbereich in der Registerkarte **Richtlinien** die Richtlinie des Administrationsagenten aus. Öffnen Sie das Eigenschaftenfenster der ausgewählten Richtlinie.

   - Um ein Verbindungsprofil für ein bestimmtes Gerät innerhalb der Gruppe zu erstellen, wählen Sie im Arbeitsbereich in der Registerkarte **Geräte** das entsprechende Gerät aus und gehen Sie wie folgt vor:

     a. Öffnen Sie das Eigenschaftenfenster des ausgewählten Geräts.

     b. Wählen Sie im Eigenschaftenfenster des Geräts im Abschnitt **Programme** den erforderlichen Administrationsagenten aus.

     c. Öffnen Sie das Eigenschaftenfenster des Administrationsagenten.

3. Klicken Sie im Eigenschaftenfenster im Abschnitt **Konnektivität** auf den Unterabschnitt **Verbindungsprofile**.

4. Klicken Sie in der Einstellungsgruppe **Verbindungsprofile des Administrationsservers** auf **Hinzufügen**.

   Standardmäßig enthält die Liste der Verbindungsprofile die Profile <Autonomer-Modus> und <Home-Administrationsserver>. Diese Profile können nicht geändert oder gelöscht werden.

   Im Profil <Autonomer-Modus> ist kein Server für die Verbindung angegeben. Daher versucht der Administrationsagent beim Umschalten auf dieses Profil nicht, eine Verbindung zu einem Administrationsserver herzustellen, während auf Client-Geräten installierte Programme in der Richtlinie für mobile Benutzer ausgeführt werden. Das Profil <Autonomer-Modus> wird übernommen, wenn die Geräte vom Netzwerk getrennt sind.

   Im Profil <Home-Administrationsserver> ist die Verbindung für den Server angegeben, der bei der Installation des Administrationsagenten festgelegt wurde. Das Profil <Home-Administrationsserver> wird verwendet, wenn ein Gerät in einem anderen Netzwerk erneut eine Verbindung zum Home-Administrationsserver herstellt.

5. Passen Sie im folgenden Fenster **Neues Profil** die Einstellungen des Verbindungsprofils an:

   - **Profilname**

     In diesem Eingabefeld können Sie sich den Namen des Verbindungsprofils anzeigen lassen oder ihn ändern.

   - **Administrationsserver**

     Adresse des Administrationsservers, zu dem das Client-Gerät eine Verbindung bei der Aktivierung des Profils herstellen soll.

   - **Port**

     Nummer des Ports, über den die Verbindung erfolgt.

   - **SSL-Port**

     Nummer des Ports, wenn die Verbindung mit dem SSL-Protokoll erfolgt.

- **SSL verwenden**

  Wenn Sie die Option aktivieren, erfolgt die Verbindung über einen gesicherten Port (mit SSL-Protokoll).

  Diese Option ist standardmäßig aktiviert. Wir empfehlen, diese Option nicht zu deaktivieren, damit Ihre Verbindung gesichert bleibt.

- Klicken Sie auf den Link **Verbindung über Proxyserver konfigurieren**, um die Verbindung über einen Proxyserver anzupassen. Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

  - **Proxyserver-Adresse**

    Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center mit dem Internet.

  - **Port**

    Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center hergestellt wird.

  - **Authentifizierung am Proxyserver**

    Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

    Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver verwenden** aktiviert ist.

  - **Benutzername** (Das Feld ist verfügbar, wenn die Option **Authentifizierung am Proxyserver** aktiviert ist)

    Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

  - **Kennwort** (Das Feld ist verfügbar, wenn die Option **Authentifizierung am Proxyserver** aktiviert ist)

    Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

    Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

- **Einstellungen des Verbindungs-Gateways**

  Gateway-Adresse, über die Client-Geräte mit dem Administrationsserver verbunden werden.

- **Modus für mobile Benutzer aktivieren**

  Wenn diese Option aktiviert ist, und eine Verbindung über dieses Profil besteht, verwenden Programme, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte im Modus für mobile Benutzer sowie Richtlinien für mobile Benutzer. Wurde für die Anwendung keine Richtlinie für mobile Benutzer definiert, verwendet die Anwendung die aktive Richtlinie.

  Wenn diese Option deaktiviert ist, wenden die Anwendungen die aktiven Richtlinien an.

  Diese Option ist standardmäßig deaktiviert.

- **Nur für Update-Download verwenden**

  Wenn diese Option aktiviert ist, wird das Profil nur beim Update-Download von den auf dem Client-Gerät installierten Programmen verwendet. Bei den übrigen Vorgängen erfolgt eine Verbindung mit dem Administrationsserver mit den ursprünglichen Verbindungseinstellungen, die bei der Installation des Administrationsagenten eingegeben wurden.

Diese Option ist standardmäßig aktiviert.

- **Verbindungseinstellungen mit den Einstellungen für den Administrationsserver synchronisieren, die in diesem Profil angegeben sind**

  Wenn diese Option aktiviert ist, stellt der Administrationsagent eine Verbindung zum Administrationsserver her und verwendet dazu die Einstellungen, die in den Profileigenschaften angegeben sind.

  Wenn diese Option deaktiviert ist, stellt der Administrationsagent eine Verbindung zum Administrationsserver mithilfe der bei der Installation angegebenen ursprünglichen Einstellungen her.

  Diese Option ist verfügbar, wenn die Option **Nur für Update-Download verwenden** deaktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

6. Aktivieren Sie die Option **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**, damit bei der Verbindung von Programmen, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte, die sich im Modus für mobile Benutzer befinden, verwendet werden und die mobile Richtlinie verwendet wird, wenn der Administrationsserver nicht verfügbar ist. Wurde für das Programm keine Richtlinie für mobile Benutzer definiert, verwendet das Programm die aktive Richtlinie.

Für mobiler Benutzer wird ein Profil zur Verbindung des Administrationsagenten zum Administrationsserver erstellt. Wird mit diesem Profil eine Verbindung des Administrationsagenten zum Administrationsserver hergestellt, so verwenden die auf dem Client-Gerät installierten Programme Richtlinien für Geräte, die sich im Modus für mobile Benutzer befinden, oder mobile Richtlinien.

Über das Umschalten eines Administrationsagenten auf einen anderen Administrationsserver

Bei der Installation des Administrationsagenten werden die ursprünglichen Verbindungseinstellungen des Administrationsagenten mit dem Administrationsserver eingegeben. Um den Administrationsagenten auf andere Administrationsserver umzuschalten, können Sie die Umschaltregeln verwenden. Diese Funktion wird nur für Administrationsagenten unterstützt, die auf Geräten unter Windows oder macOS installiert sind.

Die Umschaltregeln können durch eine Änderung der folgenden Netzwerkeigenschaften ausgelöst werden:

- Adresse des Standard-Gateways.
- IP-Adresse des DHCP-Servers (Dynamic Host Configuration Protocol).
- DNS-Suffix des Subnetzes.
- IP-Adresse des DNS-Servers des Netzwerks.
- Verfügbarkeit der Windows-Domäne. Dieser Parameter ist nur auf Windows-Geräten verfügbar.
- Adresse und Maske des Subnetzes.
- IP-Adresse des WINS-Servers des Netzwerks. Dieser Parameter ist nur auf Windows-Geräten verfügbar.
- DNS- oder NetBIOS-Name des Client-Geräts.
- Verfügbarkeit der SSL-Verbindungsadresse.

Wenn Regeln für das Umschalten des Administrationsagenten auf andere Administrationsserver definiert wurden, reagiert der Administrationsagent auf die Änderungen der Netzwerkeigenschaften folgendermaßen:

- Wenn die Netzwerkeigenschaften einer der erstellten Regeln entsprechen, wird der Administrationsagent mit dem in der Regel vorgegebenen Administrationsserver verbunden. Die auf den Client-Geräten installierten Anwendungen wechseln zu den Richtlinien für mobile Benutzer, wenn dies durch eine Regel vorgegeben wurde.
- Wird keine Regel ausgeführt, wird der Administrationsagent auf die ursprünglichen Verbindungseinstellungen mit dem Administrationsserver zurückgesetzt, die bei der Installation vorgegeben wurden. Die auf den Client-Geräten installierten Programme werden auf die aktiven Richtlinien zurückgesetzt.
- Ist der Administrationsserver nicht verfügbar, verwendet der Administrationsagent die Richtlinien für mobile Benutzer.

Der Administrationsagent verwendet die Richtlinie für mobile Benutzer nur dann, wenn die Option **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist** in den Einstellungen des Administrationsagenten aktiviert ist.

Die Verbindungseinstellungen des Administrationsagenten mit dem Administrationsserver werden im Verbindungsprofil gespeichert. Im Verbindungsprofil können Sie Regeln für den Wechsel der Client-Geräte zu den Richtlinien für mobile Benutzer erstellen sowie das Profil so einrichten, dass es nur zum Download von Updatedateien verwendet wird.

Erstellen der Regel für die Umstellung des Administrationsagenten gemäß dem Netzwerkspeicherort

Die Umstellung des Administrationsagenten gemäß des Netzwerkspeicherorts ist nur auf Geräten verfügbar, die unter Windows und macOS laufen.

Um eine Regel für die Umstellung des Administrationsagenten von einem Administrationsserver auf einen anderen bei geänderten Eigenschaften des Netzwerks anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus, für deren Geräte eine Regel für die Umstellung des Administrationsagenten gemäß der Beschreibung des Netzwerkspeicherorts erstellt werden soll.
2. Führen Sie eine der folgenden Aktionen aus:
   - Um eine Regel für alle Geräte der Gruppe zu erstellen, wählen Sie im Arbeitsbereich der Gruppe in der Registerkarte **Richtlinien** die Richtlinie des Administrationsagenten aus. Öffnen Sie das Eigenschaftenfenster der ausgewählten Richtlinie.
   - Um eine Regel für ein bestimmtes Gerät innerhalb der Gruppe zu erstellen, wählen Sie im Arbeitsbereich in der Registerkarte **Geräte** das entsprechende Gerät aus und gehen Sie wie folgt vor:
     a. Öffnen Sie das Eigenschaftenfenster des ausgewählten Geräts.
     b. Wählen Sie im Eigenschaftenfenster des Geräts im Abschnitt **Programme** den erforderlichen Administrationsagenten aus.
     c. Öffnen Sie das Eigenschaftenfenster des Administrationsagenten.

3. Klicken Sie im folgenden Fenster **Eigenschaften** im Abschnitt **Konnektivität** auf den Unterabschnitt **Verbindungsprofile**.

4. Klicken Sie im Abschnitt **Einstellungen des Netzwerkstandorts** auf **Hinzufügen**.

5. Passen Sie im folgenden Fenster **Neue Beschreibung** Sie die Einstellungen der Beschreibungen des Netzwerkspeicherorts und der Regel der Umschaltung an. Passen Sie die folgenden Einstellungen der Beschreibungen des Netzwerkspeicherorts an:

   - **Name der Beschreibungen des Netzwerkspeicherorts**

     Der Name der Beschreibungen des Netzwerkspeicherorts darf nicht mehr als 255 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\/:|).

   - **Folgendes Verbindungsprofil verwenden**

     In dieser Dropdown-Liste können Sie ein Verbindungsprofil des Administrationsagenten mit dem Administrationsserver auswählen. Das Profil wird beim Ausführen der Bedingungen der Beschreibungen des Netzwerkspeicherorts verwendet. Das Verbindungsprofil umfasst die Verbindungen des Administrationsagenten für den Administrationsserver und bestimmt den Wechsel der Client-Geräte auf mobile Richtlinien. Das Profil wird nur zum Download von Updates verwendet.

6. Klicken Sie im Block **Umschaltbedingungen** auf die Schaltfläche **Hinzufügen**, um die Liste der Bedingungen der Beschreibungen des Netzwerkspeicherorts anzulegen.

   Die Bedingungen in der Regel beruhen auf dem logischen UND-Operator. Damit die Regel zur Umschaltung gemäß der Beschreibung des Netzwerkspeicherorts ausgelöst wird, müssen alle Umschaltbedingungen der Regel erfüllt sein.

7. Wählen Sie in der Dropdown-Liste den entsprechenden Wert für die Eigenschaften des Netzwerks aus, mit dem das Client-Gerät verbunden ist:

   - **Standardmäßige Verbindungs-Gateway-Adresse** – Änderung des Standard-Gateways im Netzwerk.
   - **Adresse des DHCP-Servers** – Änderung der IP-Adresse für den DHCP-Server (Dynamic Host Configuration Protocol) im Netzwerk.
   - **DNS-Domäne** – Änderung des DNS-Suffixes im Subnetz.
   - **Adresse des DNS-Servers** – Änderung der IP-Adresse für den DNS-Server im Netzwerk.
   - **Verfügbarkeit der Windows-Domäne (nur Windows)** – Änderung des Status der Windows-Domäne, mit der das Client-Gerät verbunden ist. Verwenden Sie diese Einstellung nur für Windows-Geräte.
   - **Subnetz** – Änderung der Adresse und Subnetzmaske.
   - **Adresse des WINS-Servers (nur Windows)** – Änderung der IP-Adresse für den DNS-Server im Netzwerk. Verwenden Sie diese Einstellung nur für Windows-Geräte.
   - **Auflösbarkeit von Namen** – Änderung des DNS- oder NetBIOS-Namens des Client-Geräts.
   - **Verfügbarkeit der SSL-Verbindungsadresse** – Das Client-Gerät kann oder kann nicht (in Abhängigkeit der von Ihnen gewählten Option) eine SSL-Verbindung zu einem Server (Name:Port) herstellen. Sie können für jeden Server ein zusätzliches SSL-Zertifikat hinzufügen. In diesem Fall verifiziert der Administrationsagent das Serverzertifikat zusätzlich zur Prüfung auf eine mögliche SSL-Verbindung. Wenn das Zertifikat nicht übereinstimmt, schlägt die Verbindung fehl. Die Verbindungshäufigkeit beträgt einmal pro Minute.

8. Im folgenden Fenster können Sie einen Wert für die Umschaltbedingungen des Administrationsagenten auf einen anderen Administrationsserver angeben. Der Name des Fensters hängt von der Auswahl des Wertes während des vorhergehenden Schrittes ab. Passen Sie die folgenden Einstellungen der Umschaltbedingungen an:

   - **Wert**

     In diesem Feld können Sie einen oder mehrere Werte für die zu erstellende Bedingung hinzufügen.

   - **Wenn sie auf mindestens einen Listenwert zutrifft**

     Bei Auswahl dieser Option wird die Bedingung für jeden in der Liste **Wert** angegebenen Wert erfüllt.

     Diese Variante ist standardmäßig ausgewählt.

   - **Wenn sie auf keinen Listenwert zutrifft**

     Bei Auswahl dieser Option wird die Bedingung erfüllt, wenn ihr Wert in der Liste **Wert** nicht vorhanden ist.

9. Aktivieren Sie im Fenster **Neue Beschreibung** die Option **Beschreibung aktiv**, um die Verwendung der neuen Beschreibungen des Netzwerkspeicherorts zu aktivieren.

Daraufhin wird eine Regel zur Umschaltung gemäß der Beschreibung des Netzwerkspeicherorts erstellt, und der Administrationsagent verwendet bei Erfüllung der Bedingungen das in der Beschreibung angegebene Verbindungsprofil für die Verbindung mit dem Administrationsserver.

Die Beschreibungen des Netzwerkspeicherorts werden in der Reihenfolge, in der sie in der Liste aufgeführt sind, auf Übereinstimmung mit den Netzwerkeigenschaften überprüft. Wenn die Netzwerkeigenschaften mehreren Regeln entsprechen, wird die erste Beschreibung übernommen. Sie können die Reihenfolge der Regeln in der Liste mithilfe der Schaltflächen **Aufwärts** (↑) und **Abwärts** (↓) ändern.

Ereignisbenachrichtigungen

Dieser Abschnitt beschreibt die Auswahl der Benachrichtigungen des Administrators über die Ereignisse auf Client-Geräten sowie die Konfiguration der Benachrichtigungen zu Ereignissen.

Außerdem beschreibt er, wie der Versand von Benachrichtigungen zu Ereignissen mithilfe des Testvirus Eicar getestet werden kann.

Benachrichtigungseinstellungen für Ereignisse anpassen

Kaspersky Security Center ermöglicht die Auswahl der Benachrichtigungsmethode für Ereignisse für den Administrator auf den Client-Geräten und die Anpassung der Benachrichtigungseinstellungen:

- E-Mail. Beim Auftreten eines Ereignisses sendet das Programm Benachrichtigungen an die angegebenen E-Mail-Adressen. Der Text der Benachrichtigung kann angepasst werden.
- SMS. Beim Auftreten eines Ereignisses sendet das Programm Benachrichtigungen an die angegebenen Telefonnummern. Sie können die SMS-Benachrichtigungen konfigurieren, die über das Mail Gateway gesendet werden.
- Ausführbare Datei Beim Auftreten eines Ereignisses auf dem Gerät wird auf dem Administrator-Arbeitsplatz eine ausführbare Datei gestartet. Mithilfe der ausführbaren Datei erhält der Administrator die Parameter des eingetretenen Ereignisses.

Um die Einstellungen für Benachrichtigungen über Ereignisse auf den Client-Geräten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Klicken Sie auf den Link **Benachrichtigungseinstellungen und Ereignis-Export anpassen** und wählen Sie in der Dropdown-Liste die Option **Benachrichtigungseinstellungen anpassen**.

   Daraufhin wird das Fenster **Eigenschaften: Ereignisse** geöffnet.
4. Wählen Sie im Abschnitt **Benachrichtigung** eine Benachrichtigungsmethode aus (E-Mail, SMS, Start einer ausführbaren Datei) und passen Sie die Benachrichtigungseinstellungen an:

   - **E-Mail**

     Auf der Registerkarte **E-Mail** können Sie die E-Mail-Benachrichtigung für Ereignisse konfigurieren.

     Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen.

     Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

     - IPv4- oder IPv6-Adresse
     - Windows-Netzwerkname (NetBIOS-Name) des Geräts
     - DNS-Name des SMTP-Servers

     Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig wird Portnummer 25 verwendet.

Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren, können Sie mehrere MX-Einträge von IP-Adressen für denselben DNS-Namen des SMTP-Servers verwenden. Der gleiche DNS-Name kann mehrere MX-Einträge mit unterschiedlichen Prioritäten für das Empfangen von E-Mail-Nachrichten enthalten. Der Administrationsserver versucht, entsprechend der Priorität der MX-Einträge, die E-Mail-Nachrichten in aufsteigender Reihenfolge an den SMTP-Server zu senden. Diese Option ist standardmäßig deaktiviert.

Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren und die Verwendung von TLS-Einstellungen deaktivieren, ist es empfehlenswert, die DNSSEC-Einstellungen auf Ihrem Servergerät als zusätzliche Schutzmaßnahme beim Senden von E-Mail-Nachrichten zu verwenden.

Klicken Sie auf den Link **Einstellungen**, um zusätzliche Benachrichtigungseinstellungen zu definieren:

- Betreff (Betreff einer E-Mail-Nachricht)
- E-Mail-Adresse des Absenders
- ESMTP-Authentifizierungseinstellungen

Sie müssen ein Konto für die Authentifizierung auf einem SMTP-Server angeben, wenn die Option zur ESMTP-Authentifizierung für dem SMTP-Server aktiviert ist.

- TLS-Einstellungen für den SMTP-Server:
  - **Kein TLS verwenden**

    Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

  - **TLS verwenden, wenn vom SMTP-Server unterstützt**

    Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

  - **TLS immer verwenden und Serverzertifikat auf Gültigkeit prüfen**

    Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **TLS immer verwenden und Serverzertifikat auf Gültigkeit prüfen** auswählen, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können die TLS-Einstellungen für einen SMTP-Server angeben:

- Geben Sie eine Datei mit SMTP-Server-Zertifikat an:

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center prüft, ob das Zertifikat eines SMTP-Servers auch von eine vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

- Geben Sie die Datei des Client-Zertifikats an:

Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen Zertifizierungsstelle. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

- X-509-Zertifikat:

Sie müssen eine Datei mit dem Zertifikat und eine Datei mit dem privaten Schlüssel angeben. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Laden der Dateien ist spielt keine Rolle. Wenn beide Dateien geladen sind, müssen Sie das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- pkcs12-Container:

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

Das Feld **Benachrichtigungstext** enthält Standard-Text mit der Information zum Ereignis, der beim Eintreten des Ereignisses versendet wird. Dieser Text enthält Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne. Sie können den Text der Meldung bearbeiten und weitere Platzhalter mit relevanten Informationen über das Ereignis hinzufügen. Klicken Sie auf die Schaltfläche rechts neben dem Feld, um eine Liste mit verfügbaren Platzhaltern anzuzeigen.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Klicken Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren**, um die maximale Anzahl an Benachrichtigungen anzugeben, die das Programm während des angegebenen Zeitintervalls versenden darf.

Klicken Sie auf die Schaltfläche **Testnachricht senden**, um zu überprüfen, ob Sie die Benachrichtigungen richtig konfiguriert haben. Das Programm sollte eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen senden.

- **SMS**

Auf der Registerkarte **SMS** können Sie den Versand von SMS-Benachrichtigungen zu verschiedenen Ereignissen an ein Mobiltelefon anpassen. SMS-Nachrichten werden über ein Mail-Gateway gesendet.

Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen ein, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen. Die Benachrichtigungen werden an die Telefonnummern gesendet, die den angegebenen E-Mail-Adressen zugewiesen sind.

Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- Windows-Netzwerkname (NetBIOS-Name) des Geräts
- DNS-Name des SMTP-Servers

Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Ports für die Kommunikation eines SMTP-Servers an. Standardmäßig wird Portnummer 25 verwendet.

Klicken Sie auf den Link **Einstellungen**, um zusätzliche Benachrichtigungseinstellungen zu definieren:

- Betreff (Betreff einer E-Mail-Nachricht)
- E-Mail-Adresse des Absenders
- ESMTP-Authentifizierungseinstellungen

Falls erforderlich, können Sie ein Konto für die Authentifizierung auf einem SMTP-Server angeben, wenn die Option zur ESMTP-Authentifizierung für einen SMTP-Server aktiviert ist.

- TLS-Einstellungen für einen SMTP-Server

Sie können entweder die Verwendung von TLS deaktivieren, TLS verwenden, wenn der SMTP-Server dieses Protokoll unterstützt, oder die Verwendung von TLS erzwingen. Wenn Sie nur TLS verwenden möchten, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie in dem Fall, dass Sie nur TLS verwenden möchten, ein Zertifikat für die Client-Authentifizierung am SMTP-Server angeben.

- Geben Sie eine Datei mit SMTP-Server-Zertifikat an

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von einer vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei in Kaspersky Security Center hochladen. Kaspersky Security Center prüft, ob das Zertifikat des SMTP-Servers auch von einer vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu dem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von einer vertrauenswürdigen Zertifizierungsstelle kommt.

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist. Das Feld **Benachrichtigungstext** enthält Standard-Text mit der Information zum Ereignis, der beim Eintreten des Ereignisses versendet wird. Dieser Text enthält Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne. Sie können den Text der Meldung bearbeiten und weitere Platzhalter mit relevanten Informationen über das Ereignis hinzufügen. Klicken Sie auf die Schaltfläche rechts neben dem Feld, um eine Liste mit verfügbaren Platzhaltern anzuzeigen.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Klicken Sie auf den Link **Beschränkung für Anzahl der Benachrichtigungen konfigurieren**, um die maximale Anzahl an Benachrichtigungen anzugeben, die das Programm während des angegebenen Zeitintervalls versenden darf.

Klicken Sie auf die Schaltfläche **Testnachricht senden** um zu überprüfen, ob Sie die Benachrichtigungen richtig konfiguriert haben. Das Programm sollte eine Testnachricht an den von Ihnen angegebenen Empfänger senden.

- **Start einer ausführbaren Datei**

  Wenn diese Methode der Zustellung von Benachrichtigungen ausgewählt ist, können Sie im Eingabefeld das Programm angeben, das gestartet wird, sobald ein Ereignis eintritt.

  Wenn Sie auf den Link **Beschränkung für Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, die das Programm innerhalb des angegebenen Zeitintervalls versenden darf.

  Klicken Sie auf die Schaltfläche **Testnachricht senden**, um zu prüfen, ob Sie die Benachrichtigungen korrekt konfiguriert haben: Das Programm sendet dann eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen.

5. Geben Sie im Feld **Benachrichtigungstext** den Text ein, den das Programm bei Eintreten eines Ereignisses versenden wird.

   Aus der Dropdown-Liste rechts vom Textfeld können in die Nachricht Platzhalter für zusätzliche Einstellungen mit den Ereignisdetails (wie Beschreibung, Eintrittszeit des Ereignisses und sonstiges) hinzugefügt werden.

   Wenn der Benachrichtigungstext das Zeichen % enthält, muss es zweimal angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

6. Überprüfen Sie über die Schaltfläche **Testnachricht senden**, ob die Benachrichtigungen richtig eingestellt wurden.

   Das Programm sendet eine Testbenachrichtigung an den angegebenen Empfänger.

7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Daraufhin werden die angepassten Einstellungen der Benachrichtigung auf alle Ereignisse übernommen, die auf den Client-Geräten auftreten.

Sie können die Benachrichtigungseinstellungen für bestimmte Ereignisse im Abschnitt **Konfiguration von Ereignissen** in den Einstellungen des Administrationsservers für eine Richtlinieneinstellung oder eine Programmeinstellung überschreiben.

Verteilung von Benachrichtigungen prüfen

Zur Prüfung der Verteilung von Benachrichtigungen über Ereignisse wird eine Benachrichtigung über den Fund eines Test-"Virus" Eicar auf den Client-Geräten verwendet.

Um die Verteilung von Benachrichtigungen über Ereignisse zu überprüfen, gehen Sie wie folgt vor:

1. Beenden Sie auf dem Client-Computer die Aufgabe zum Echtzeitschutz für Dateien, und kopieren Sie den Test-"Virus" Eicar auf das Client-Gerät. Aktivieren Sie die Aufgabe zum Echtzeitschutz für Dateien wieder.

2. Starten Sie die Untersuchungsaufgabe für die Client-Geräte in einer Administrationsgruppe oder für eine Reihe von Geräten, zu denen das Client-Gerät mit dem Test-"Virus" Eicar gehört.

   Wenn die Untersuchungsaufgabe richtig angepasst wurde, wird der Test-"Virus" bei der Ausführung der Aufgabe gefunden. Wurden die Einstellungen für Benachrichtigungen richtig angepasst, empfangen Sie eine Meldung über den gefundenen Virus.

   Im Arbeitsbereich des Knotens **Administrationsserver** wird auf der Registerkarte **Ereignisse** in der Auswahl **Letzte Ereignisse** eine Liste mit Einträgen über gefundene "Viren" angezeigt.

Der Test-"Virus" Eicar enthält keinen Programmcode, der Ihrem Gerät Schaden zufügen könnte. Die meisten Sicherheitsanwendungen von Herstellern identifizieren ihn als Virus. Der Test-"Virus" steht auf der offiziellen Seite der EICAR-Organisation zum Download bereit.

Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei

Kaspersky Security Center bietet die Möglichkeit, den Administrator durch den Start einer ausführbaren Datei über Ereignisse auf den Client-Geräten zu benachrichtigen. Diese ausführbare Datei muss eine weitere ausführbare Datei mit Parameterplatzhaltern für das Ereignis enthalten, die dem Administrator übermittelt werden müssen (siehe Abbildung unten).

Parameterplatzhalter zur Beschreibung des Ereignisses

Parameterplatzhalter	Beschreibung des Parameterplatzhalters
%SEVERITY%	Signifikanz des Ereignisses. Mögliche Werte: • **Information** • **Warnung** • **Fehler** • **Kritisch**
%COMPUTER%	Name des Geräts, auf dem das Ereignis eingetreten ist. Die maximale Länge des Gerätenamens beträgt 256 Zeichen.
%DOMAIN%	Domänenname des Geräts, auf dem das Ereignis eingetreten ist.
%EVENT%	Name des Ereignistyps. Die maximale Länge des Namens des Ereignistyps beträgt 50 Zeichen.
%DESCR%	Ereignisbeschreibung. Die maximale Länge der Beschreibung beträgt 1000 Zeichen.
%RISE_TIME%	Zeitpunkt der Ereigniserstellung.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Aufgabenname. Die maximale Länge des Aufgabennamens beträgt 100 Zeichen.
%KL_PRODUCT%	Name der Anwendung.
%KL_VERSION%	Versionsnummer der Anwendung.
%KLCSAK_EVENT_SEVERITY_NUM%	Signifikanzkennzahl des Ereignisses. Mögliche Werte: • 1 – **Information** • 2 – **Warnung** • 3 – **Fehler** • 4 – **Kritisch**
%HOST_IP%	IP-Adresse des Geräts, auf dem das Ereignis eingetreten ist.
%HOST_CONN_IP%	IP-Adresse der Verbindung auf dem Geräts, auf dem das Ereignis eingetreten ist.

Beispiel:
Ausführbare Datei zur Benachrichtigung über Ereignisse (z. B. script1.bat), innerhalb der eine weitere ausführbare Datei (z. B. script2.bat) mit dem Parameterplatzhalter %COMPUTER% gestartet wird. Beim Auftreten eines Ereignisses auf dem Gerät des Administrators wird die Datei script1.bat gestartet, die wiederum die Datei script2.bat mit dem Parameter %COMPUTER% startet. Dadurch erhält der Administrator den Namen des Geräts, auf dem das Ereignis aufgetreten ist.

Kommunikation mit TLS verschlüsseln

Um Schwachstellen im Unternehmensnetzwerk Ihres Unternehmens zu beheben, können Sie die Datenverkehrsverschlüsselung mittels TLS-Protokoll aktivieren. Sie können die TLS-Verschlüsselungsprotokolle und die unterstützten Cipher-Suites auf dem Administrationsserver und dem iOS MDM Server aktivieren. Kaspersky Security Center unterstützt das TLS-Protokoll in den Versionen 1.0, 1.1, 1.2 und 1.3. Sie können die erforderlichen Verschlüsselungsprotokolle und Cipher-Suites auswählen.

Kaspersky Security Center verwendet selbstsignierte Zertifikate. Zusätzliche Konfiguration der iOS-Geräte ist nicht erforderlich. Sie können auch Ihre eigenen Zertifikate verwenden. Die Experten von Kaspersky empfehlen, Zertifikate zu verwenden, die von vertrauenswürdigen Zertifizierungsstellen erteilt wurden.

Administrationsserver

So konfigurieren Sie die erlaubten Verschlüsselungsprotokolle und Cipher-Suites auf dem Administrationsserver:

1. Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

2. Verwenden Sie das Flag "SrvUseStrictSslSettings", um erlaubte Verschlüsselungsprotokolle und Cipher-Suites auf dem Administrationsserver zu konfigurieren. Geben Sie den folgenden Befehl ein:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <Wert> -t d
   ```

   Geben Sie den Parameter "<Wert>" des Flags "SrvUseStrictSslSettings" an:

   - `4` – Es sind nur die Protokolle TLS 1.2 und TLS 1.3 aktiviert. Außerdem sind Cipher-Suites mit TLS_RSA_WITH_AES_256_GCM_SHA384 aktiviert (Diese Cipher-Suites werden für die Abwärtskompatibilität mit früheren Versionen von Kaspersky Security Center benötigt). Dies ist der Standardwert.

     Für das Protokoll TLS 1.2 unterstützte Cipher-Suites:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (Cipher-Suite mit TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Für das Protokoll TLS 1.3 unterstützte Cipher-Suites:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5` – Es sind nur die Protokolle TLS 1.2 und TLS 1.3 aktiviert. Für die Protokolle TLS 1.2 und TLS 1.3 werden die unten aufgeführten Cipher-Suites unterstützt.

     Für das Protokoll TLS 1.2 unterstützte Cipher-Suites:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Für das Protokoll TLS 1.3 unterstützte Cipher-Suites:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Es wird nicht empfohlen, "0", "1", "2" oder "3" als Parameterwert für das Flag "SrvUseStrictSslSettings" zu verwenden. Diese Parameterwerte stehen für unsichere Versionen des TLS-Protokolls (die Protokolle TLS 1.0 und TLS 1.1) und unsichere Cipher-Suites. Sie werden nur aus Gründen der Abwärtskompatibilität mit älteren Versionen von Kaspersky Security Center verwendet.

3. Starten Sie die folgenden Dienste von Kaspersky Security Center 15.1 neu:
   - Administrationsserver
   - Webserver
   - Aktivierungs-Proxy

Die Verschlüsselung des Datenverkehrs mithilfe des TLS-Protokolls ist aktiviert.

Sie können die Flags "KLTR_TLS12_ENABLED" und "KLTR_TLS13_ENABLED" verwenden, um die Unterstützung der Protokolle TLS 1.2 bzw. TLS 1.3 zu aktivieren. Diese Flags sind standardmäßig aktiviert.

So aktivieren oder deaktivieren Sie die Unterstützung der Protokolle TLS 1.2 und TLS 1.3:

1. Führen Sie das Tool "klscflag" aus.

   Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

2. Geben Sie einen der folgenden Befehle mit Administratorrechten in die Windows-Eingabeaufforderung ein:
   - Verwenden Sie diesen Befehl, um die Unterstützung des Protokolls TLS 1.2 zu aktivieren oder zu deaktivieren:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <Wert> -t d
     ```

   - Verwenden Sie diesen Befehl, um die Unterstützung des Protokolls TLS 1.3 zu aktivieren oder zu deaktivieren:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <Wert> -t d
     ```

Geben Sie den Parameter <Wert> des Flags an:

- `1` – Die Unterstützung des TLS-Protokolls ist aktiviert.
- `0` – Die Unterstützung des TLS-Protokolls ist deaktiviert.

iOS MDM-Server

Die Verbindung zwischen den iOS-Geräten und dem iOS MDM-Server ist standardmäßig verschlüsselt.

Um zugelassene Verschlüsselungsprotokolle und Cipher-Suites auf dem iOS MDM-Server anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie die Systemregistrierung des Client-Geräts, auf dem der iOS MDM-Server installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** → **Ausführen**.
2. Rufen Sie den folgenden Abschnitt auf:
   - Für 32-Bit-Systeme:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - Für 64-Bit-Systeme:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Erstellen Sie einen Schlüssel mit dem Namen `StrictSslSettings`.
4. Geben Sie als Schlüsseltyp `DWORD` an.
5. Legen Sie den Wert des Schlüssels fest:
   - `2` – Die Protokolle TLS 1.0, TLS 1.1 und TLS 1.2 sind aktiviert.
   - `3` – Es ist nur das Protokoll TLS 1.2 aktiviert (Standardwert).
6. Starten Sie den Dienst des iOS MDM-Servers von Kaspersky Security Center neu.

Konfiguration der Schnittstelle

Sie können die Benutzeroberfläche von Kaspersky Security Center konfigurieren:

- Ein- und Ausblenden von Objekten der Konsolenstruktur, im Arbeitsbereich und in den Eigenschaftenfenstern von Objekten (Ordner, Abschnitte), abhängig von den verwendeten Funktionen.
- Elemente des Hauptfensters ein- und ausblenden (z. B. die Konsolenstruktur oder Standardmenüs wie **Aktionen** und **Ansicht**).

So konfigurieren Sie die Benutzeroberfläche von Kaspersky Security Center-Oberfläche gemäß den derzeit verwendeten Funktionen:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie in der Menüleiste des Programmhauptfensters den Punkt **Ansicht → Benutzeroberfläche anpassen**.
3. Konfigurieren Sie in dem sich öffnenden Fenster **Einstellungen der Benutzeroberfläche** die Darstellung von Elementen der Benutzeroberfläche mit den folgenden Kontrollkästchen:

   - **Schwachstellen- und Patch-Management anzeigen**

     Wenn diese Option aktiviert ist, wird im Ordner **Remote-Installation** der Unterordner **Geräte-Images verteilen** und im Ordner **Datenverwaltung** der Unterordner **Hardware** angezeigt.

     Diese Option ist standardmäßig deaktiviert, wenn der Schnellstartassistent noch nicht abgeschlossen ist. Diese Option ist standardmäßig aktiviert, nachdem der Schnellstartassistent abgeschlossen wurde.

     > Bei aktivierter Option sind die Menüpunkte **RDP-Sitzung erstellen** und **Windows Desktopfreigabe** auch dann nicht verfügbar, wenn Sie eine Lizenz zur Systemverwaltung verwenden.

   - **Verschlüsselung und Datenschutz anzeigen**

     Wenn diese Option aktiviert ist, wird in der Konsolenstruktur der Ordner **Verschlüsselung und Datenschutz** angezeigt.

     Diese Option ist standardmäßig aktiviert.

   - **Einstellungen von Endpoint Control anzeigen**

     Wenn diese Option aktiviert ist, werden die folgenden Unterabschnitte im Abschnitt **Sicherheitskontrolle** des Eigenschaftenfensters der Richtlinie von Kaspersky Endpoint Security für Windows angezeigt:

     - **Programmkontrolle**
     - **Gerätekontrolle**
     - **Web-Kontrolle**
     - **Adaptive Kontrolle von Anomalien**

     Wenn diese Option deaktiviert ist, werden die oben angegebenen Unterabschnitte im Abschnitt **Sicherheitskontrolle** nicht angezeigt.

     Diese Option ist standardmäßig aktiviert.

   - **Komponente "Verwaltung mobiler Geräte" anzeigen**

     Wenn diese Option aktiviert wurde, ist die Funktion **Verwaltung mobiler Geräte** verfügbar. Nach dem Neustart des Programms wird in der Konsolenstruktur der Ordner **Mobile Geräte** angezeigt.

     Diese Option ist standardmäßig aktiviert.

   - **Sekundäre Administrationsserver anzeigen**

     Wenn das Kontrollkästchen aktiviert ist, werden in der Konsolenstruktur die Knoten der sekundären und virtuellen Administrationsserver innerhalb der Administrationsgruppen angezeigt. Die mit sekundären und virtuellen Administrationsservern verbundenen Funktionen, z. B. das Erstellen der Aufgaben zur Remote-Installation von Programmen auf sekundären Administrationsservern, sind hier verfügbar.

Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Abschnitte der Sicherheitseinstellungen anzeigen**

  Wenn diese Option aktiviert ist, wird der Abschnitt **Sicherheit** in den Eigenschaftenfenstern des Administrationsservers, der Administrationsgruppen und anderen Objekten angezeigt. Mit dieser Option können Sie Benutzern und Benutzergruppen benutzerdefinierte Berechtigungen für die Arbeit mit Objekten erteilen.

  Diese Option ist standardmäßig deaktiviert.

4. Klicken Sie auf die Schaltfläche **OK**.

Um einige der Änderungen zu übernehmen, müssen Sie das Hauptprogrammfenster schließen und anschließend erneut öffnen.

So konfigurieren Sie die Anzeige von Elementen im Hauptprogrammfenster:

1. Wählen Sie in der Menüleiste des Hauptprogrammfensters den Punkt **Ansicht** → **Konfigurieren**.
2. Konfigurieren Sie im folgenden Fenster **Ansicht anpassen** die Anzeige der Elemente des Hauptfensters mithilfe von Kontrollkästchen.
3. Klicken Sie auf die Schaltfläche **OK**.

Geräte im Netzwerk finden

In diesem Abschnitt werden Schritte beschrieben, die Sie nach der Installation von Kaspersky Security Center unternehmen müssen.

Szenario: Netzwerkgeräte finden

Die Gerätesuche muss vor der Installation einer Sicherheitsanwendung ausgeführt werden. Der Administrationsserver erhält Informationen über erkannte Geräte und ermöglicht Ihnen, die Geräte mittels Richtlinien zu verwalten. Regelmäßige Netzwerkabfragen sind erforderlich, um die Liste der im Netzwerk verfügbaren Geräte zu aktualisieren.

Stellen Sie vor dem Start der Netzwerkabfrage sicher, dass das SMB-Protokoll aktiviert ist. Andernfalls kann Kaspersky Security Center die Geräte im abgefragten Netzwerk nicht erkennen. Um das SMB-Protokoll zu aktivieren, folgen Sie der Anleitung für Ihr Betriebssystem.

Die Erkennung von Geräten im Netzwerk erfolgt in den folgenden Schritten:

1. **Geräte entdecken**

   Der Schnellstartassistenten führt Sie durch die erstmalige Gerätesuche und hilft, Geräte im Netzwerk wie z. B. Computer, Tablets und Mobiltelefone zu finden. Die Gerätesuche kann auch manuell durchgeführt werden.

2. **Geplante Abfrage konfigurieren**

   Bestimmen Sie, welche Abfragearten Sie regelmäßig verwenden möchten. Aktivieren Sie die erforderlichen Arten und konfigurieren Sie den Abfragezeitplan. Sie können sich dabei auf die Empfehlungen für die Häufigkeiten von Netzwerkabfragen beziehen.

3. **Regeln zum Hinzufügen neu entdeckter Geräte zu Administrationsgruppen einrichten (optional)**

   Wenn in Ihrem Netzwerk neue Geräte auftauchen, werden sie bei regelmäßigen Abfragen entdeckt und automatisch zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt. Sie können Verschiebungsregeln für Geräte einrichten, um die Zuordnung der Geräte zur Gruppe **Verwaltete Geräte** zu automatisieren. Darüber hinaus können Sie Aufbewahrungsregeln konfigurieren.

   Wenn Sie den Schritt 3 überspringen, werden die neu entdeckten Geräte der Gruppe **Nicht zugeordnete Geräte** zugeordnet. Bei Bedarf können Sie diese Geräte manuell in die Gruppe **Verwaltete Geräte** verschieben. Wenn Sie die Geräte manuell in die Gruppe **Verwaltete Geräte** verschieben, können Sie die Informationen zu jedem Gerät analysieren, bestimmen, ob das Gerät in eine Administrationsgruppe verschoben werden soll, und wenn ja, die entsprechende Gruppe angeben.

Ergebnisse

Der Abschluss des Szenarios bringt folgende Ergebnisse mit sich:

- Der Kaspersky Security Center Administrationsserver findet die Geräte im Netzwerk und stellt Ihnen Informationen zu diesen Geräten zur Verfügung.
- Zukünftige Abfragen werden eingerichtet und nach einem festgelegten Zeitplan ausgeführt.
- Neu entdeckte Geräte werden gemäß den konfigurierten Regeln bestimmten Gruppen zugewiesen. (Falls keine Regeln erstellt wurden, bleiben die Geräte in der Gruppe **Nicht zugeordnete Geräte**).

Nicht zugeordnete Geräte

Dieser Abschnitt enthält Informationen zur Arbeit mit Geräten im Firmennetzwerk, die nicht zur Administrationsgruppe gehören.

Suchen von Geräten

Dieser Abschnitt beschreibt die Arten der Gerätesuche, die in Kaspersky Security Center verfügbar sind, und bietet Informationen zur Verwendung jeder dieser Arten.

Der Administrationsserver erhält mittels regelmäßiger Netzwerkabfragen Informationen über die Struktur des Netzwerks und der Geräte in diesem Netzwerk. Diese Informationen werden in der Administrationsserver-Datenbank gespeichert. Der Administrationsserver kann folgende Arten von Netzwerkabfragen durchführen:

- **Windows-Netzwerkabfrage**. Der Administrationsserver kann zwei Arten von Windows-Netzwerkabfragen durchführen: schnell und vollständig. Bei der Schnellabfrage empfängt der Administrationsserver nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks. Während einer vollständigen Abfrage werden zusätzliche Informationen von jedem Client-Gerät abgefragt, z. B. Name des Betriebssystems, IP-Adresse, DNS-Name und NetBIOS-Name. Standardmäßig sind sowohl die Schnellabfrage als auch die vollständige Abfrage aktiviert. Es ist möglich, dass die Windows-Netzwerkabfrage Geräte nicht findet, wenn z. B. die Ports UDP 137, UDP 138, TCP 139 im Router oder durch die Firewall geschlossen sind.

- **Abfrage des Active Directory**. Der Administrationsserver empfängt Informationen über die Struktur der Active Directory-Gruppen sowie über die DNS-Namen der Geräte, die zu Active Directory-Gruppen gehören. Diese Art der Abfrage ist standardmäßig aktiviert. Es wird empfohlen, die Abfrage des Active Directory zu verwenden, falls Sie Active Directory verwenden; andernfalls wird der Administrationsserver keine Geräte finden. Wenn Sie Active Directory verwenden, aber einige der vernetzten Geräte nicht als Teilnehmer aufgelistet sind, dann können diese Geräte nicht durch die Abfrage des Active Directory gefunden werden.

- **IP-Bereiche durchsuchen**. Der Administrationsserver fragt die erstellten IP-Bereiche mittels ICMP-Paketen oder NBNS-Protokoll ab und ruft alle Daten über die Geräte ab, die zu den IP-Bereichen gehören. Diese Art der Abfrage ist standardmäßig deaktiviert. Es wird nicht empfohlen, diese Art der Abfrage zu verwenden, wenn Sie die Windows-Netzwerkabfrage und/oder die Abfrage des Active Directory verwenden.

- **Zeroconf-Abfrage**. Ein Verteilungspunkt, der das IPv6-Netzwerk unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) abfragt. Diese Art der Abfrage ist standardmäßig deaktiviert. Sie können die Zeroconf-Abfrage auf Verteilungspunkten mit Linux verwenden.

Wenn Sie Verschiebungsregeln für Geräte eingerichtet und aktiviert haben, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Verwaltete Geräte** aufgenommen. Wenn keine Verschiebungsregeln aktiviert sind, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Nicht zugeordnete Geräte** aufgenommen.

Sie können die Einstellungen für die Gerätesuche für jede Art separat bearbeiten. Zum Beispiel können Sie den Abfragezeitplan ändern, oder definieren, ob die Domänengesamtstruktur oder nur eine bestimme Domäne abgefragt werden soll.

Stellen Sie vor dem Start der Netzwerkabfrage sicher, dass das SMB-Protokoll aktiviert ist. Andernfalls kann Kaspersky Security Center die Geräte im abgefragten Netzwerk nicht erkennen. Um das SMB-Protokoll zu aktivieren, folgen Sie der Anleitung für Ihr Betriebssystem.

Windows-Netzwerkabfrage

Über die Windows-Netzwerkabfrage

Bei der Schnellabfrage empfängt der Administrationsserver nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks. Bei einer vollständigen Abfrage werden von jedem Client-Gerät folgende Informationen angefordert:

- Betriebssystem-Name

- IP-Adresse

- DNS-Name
- NetBIOS-Name

Die folgenden Voraussetzungen gelten sowohl für die schnelle als auch für die vollständige Abfrage:

- Die Ports UDP 137/138, TCP 139, UDP 445, TCP 445 müssen im Netzwerk verfügbar sein.
- Das SMB-Protokoll ist aktiviert.
- Der Microsoft-Computersuchdienst muss verwendet werden, und der Computer mit dem primären Suchdienst muss auf dem Administrationsserver aktiviert sein.
- Der Microsoft-Computersuchdienst muss verwendet werden, und der Computer mit dem primären Suchdienst muss auf den Client-Geräten aktiviert sein:
  - Auf mindestens einem Gerät, wenn sich nicht mehr als 32 Geräte im Netzwerk befinden.
  - Auf mindestens einem Gerät pro 32 Geräten im Netzwerk.

Die vollständige Abfrage kann nur durchgeführt werden, wenn die Schnellabfrage mindestens einmal durchgeführt wurde.

Einstellungen der Windows-Netzwerkabfrage anzeigen und ändern

Um die Einstellungen der Windows-Netzwerkabfrage zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **Domänen**.

   Sie können zum Ordner **Gerätesuche** aus dem Ordner **Nicht zugeordnete Geräte** wechseln, indem Sie auf die Schaltfläche **Jetzt abfragen** klicken.

   Im Arbeitsbereich des Unterordners **Domänen** wird eine Liste mit Geräten angezeigt.

2. Klicken Sie auf die Schaltfläche **Jetzt abfragen**.

   Das Fenster der Domäneneigenschaften wird geöffnet. Bearbeiten Sie bei Bedarf die Einstellungen der Windows-Netzwerkabfrage:

   - **Abfrage des Windows-Netzwerks aktivieren**

     Diese Variante ist standardmäßig festgelegt. Wenn Sie keine Windows-Netzwerkabfrage durchführen möchten (z. B. weil die Abfrage des Active Directory für Sie ausreichend ist), können Sie diese Option deaktivieren.

   - **Zeitplan für schnelle Abfrage festlegen**

     Das Standardintervall beträgt 15 Minuten.

     Bei der Schnellabfrage empfängt der Administrationsserver nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks.

     Alte Daten werden vollständig durch die bei der nächsten Abfrage empfangenen Daten ersetzt.

     Folgende Varianten sind als Intervall verfügbar:

     - **Alle n Tage**

       Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Alle n Minuten**

  Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

  Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

- **Nach Wochentagen**

  Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

  Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

- **Übersprungene Aufgaben starten**

  Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

  Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

  Diese Option ist standardmäßig aktiviert.

- **Zeitplan für vollständige Abfrage festlegen**

  Das Standardabfrageintervall beträgt eine Stunde. Alte Daten werden vollständig durch die bei der nächsten Abfrage empfangenen Daten ersetzt.

  Folgende Varianten sind als Intervall verfügbar:

  - **Alle n Tage**

    Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

    Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

  - **Alle n Minuten**

    Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

    Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

  - **Nach Wochentagen**

    Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

    Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

  - **Monatlich, an angegebenen Tagen der gewählten Wochen**

Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

- **Übersprungene Aufgaben starten**

  Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

  Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

  Diese Option ist standardmäßig aktiviert.

Wenn Sie die Abfrage sofort durchführen möchten, klicken Sie auf **Jetzt abfragen**. Beide Arten der Abfrage werden gestartet.

Am virtuellen Administrationsserver können Sie im Eigenschaften-Fenster des Verteilungspunkts im Abschnitt **Gerätesuche** die Einstellungen für die Windows-Netzwerkabfrage anzeigen und ändern.

Abfrage des Active Directory

Verwenden Sie die Abfrage des Active Directory, wenn Sie Active Directory verwenden – andernfalls wird die Verwendung anderer Arten der Abfrage empfohlen. Wenn Sie Active Directory verwenden, aber einige der vernetzten Geräte nicht als Teilnehmer aufgelistet sind, können diese Geräte nicht durch die Abfrage des Active Directory gefunden werden.

Die Ergebnisse der Active Directory-Abfrage werden unabhängig von den Ergebnissen der nachfolgenden Abfragen 30 Tage lang auf dem Administrationsserver gespeichert.

Stellen Sie vor dem Start der Netzwerkabfrage sicher, dass das SMB-Protokoll aktiviert ist. Andernfalls kann Kaspersky Security Center die Geräte im abgefragten Netzwerk nicht erkennen. Um das SMB-Protokoll zu aktivieren, folgen Sie der Anleitung für Ihr Betriebssystem.

Einstellungen für die Abfrage des Active Directory anzeigen und ändern

Um die Abfrageeinstellungen der Gruppe des Active Directory zu anzeigen und ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **Active Directory**.

   Alternativ können Sie zum Ordner **Gerätesuche** aus dem Ordner **Nicht zugeordnete Geräte** wechseln, indem Sie auf die Schaltfläche **Jetzt abfragen** klicken.

2. Klicken Sie auf die Schaltfläche **Abfrageeinstellungen anpassen**.

Das Eigenschaftenfenster von Active Directory wird geöffnet. Bearbeiten Sie bei Bedarf die Einstellungen der Abfrage des Active Directory:

- **Abfrage des Active Directory zulassen**

  Diese Variante ist standardmäßig festgelegt. Wenn Sie jedoch kein Active Directory verwenden, ergibt die Abfrage keine Ergebnisse. In einem solchen Fall können Sie diese Option deaktivieren.

- **Abfragezeitplan festlegen**

  Das Standardabfrageintervall beträgt eine Stunde.

  Folgende Varianten sind als Intervall verfügbar:

  - **Alle n Tage**

    Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

    Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

  - **Alle n Minuten**

    Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

    Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

  - **Nach Wochentagen**

    Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

    Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

  - **Monatlich, an angegebenen Tagen der gewählten Wochen**

    Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

    Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

  - **Übersprungene Aufgaben starten**

    Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

    Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

    Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

    Diese Option ist standardmäßig aktiviert.

- **Erweitert**

  Sie können auswählen, welche Active Directory-Domänen abgefragt werden sollen:

  - Active Directory-Domäne, zu der das Kaspersky Security Center gehört
  - Domänengesamtstruktur, zu der das Kaspersky Security Center gehört
  - Festgelegte Liste von Active Directory-Domänen.

Bei Auswahl dieser Option können Sie Domänen zum Abfragebereich hinzufügen:

- Klicken Sie auf die Schaltfläche **Hinzufügen**.
- Geben Sie in den entsprechenden Feldern die Adresse des Domänencontrollers sowie den Namen und das Kennwort des darauf zugreifenden Benutzerkontos an.
- Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Sie können die Adresse des Domänencontrollers in der Liste auswählen und auf **Ändern** oder **Entfernen** klicken, um die Adresse zu ändern oder zu entfernen.

- Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Wenn Sie die Abfrage sofort durchführen möchten, klicken Sie auf die Schaltfläche **Jetzt abfragen**.

Am virtuellen Administrationsserver können Sie im Eigenschaften-Fenster des Verteilungspunkts im Abschnitt **Gerätesuche** die Einstellungen für die Abfrage des Active Directory-Gruppen anzeigen und ändern.

IP-Bereiche abfragen

Der Administrationsserver fragt die erstellten IP-Bereiche mittels ICMP-Paketen oder NBNS-Protokoll ab und ruft alle Daten über die Geräte ab, die zu den IP-Bereichen gehören. Diese Art der Abfrage ist standardmäßig deaktiviert.

Geben Sie für alle Linux-basierten Hosts innerhalb eines Microsoft Active Directory- oder Samba-Domänencontrollers den `netbios name` und die `workgroup` in der Datei `/etc/samba/smb.conf` an. Andernfalls können Hosts mehrfach in den Abfrageergebnissen enthalten sein.

Stellen Sie vor dem Start der Netzwerkabfrage sicher, dass das SMB-Protokoll aktiviert ist. Andernfalls kann Kaspersky Security Center die Geräte im abgefragten Netzwerk nicht erkennen. Um das SMB-Protokoll zu aktivieren, folgen Sie der Anleitung für Ihr Betriebssystem.

Einstellungen für die Abfrage der IP-Bereiche anzeigen und ändern

Um die Abfrageeinstellungen der Gruppe des IP-Bereichs zu anzeigen und ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **IP-Bereiche**.

   Sie können aus dem Ordner **Nicht zugeordnete Geräte** zum **Gerätesuche** wechseln. Klicken Sie dazu auf **Jetzt abfragen**.

2. Klicken Sie bei Bedarf im Unterordner **IP-Bereiche** auf **Subnetz hinzufügen**, um einen abzufragenden IP-Bereich hinzuzufügen, und klicken Sie anschließend auf **OK**.

3. Klicken Sie auf die Schaltfläche **Abfrageeinstellungen anpassen**.

Das Eigenschaftenfenster der IP-Bereiche wird geöffnet. Die Einstellungen für die Abfrage der IP-Bereiche können bei Bedarf geändert werden:

- **Abfrage des IP-Bereichs zulassen**

  Diese Variante ist standardmäßig nicht festgelegt. Es wird nicht empfohlen, diese Art der Abfrage zu verwenden, wenn Sie die Windows-Netzwerkabfrage und/oder die Abfrage des Active Directory verwenden.

- **Abfragezeitplan festlegen**

  Das Standardintervall beträgt 420 Minuten. Alte Daten werden vollständig durch die bei der nächsten Abfrage empfangenen Daten ersetzt.

  Folgende Varianten sind als Intervall verfügbar:

  - **Alle n Tage**

    Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

    Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

  - **Alle n Minuten**

    Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

    Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

  - **Nach Wochentagen**

    Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

    Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

  - **Monatlich, an angegebenen Tagen der gewählten Wochen**

    Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

    Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

  - **Übersprungene Aufgaben starten**

    Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

    Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

    Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

    Diese Option ist standardmäßig aktiviert.

Wenn Sie die Abfrage sofort durchführen möchten, klicken Sie auf **Jetzt abfragen**. Diese Schaltfläche ist nur verfügbar, wenn Sie **Abfrage des IP-Bereichs zulassen** aktiviert haben.

Am virtuellen Administrationsserver können Sie im Eigenschaften-Fenster des Verteilungspunkts im Abschnitt **Gerätesuche** die Einstellungen für die Abfrage der IP-Bereiche anzeigen und ändern. Die Client-Geräte, die während der Abfrage der IP-Bereiche gefunden wurden, werden im Ordner **Domänen** des virtuellen Administrationsservers angezeigt.

Zeroconf-Abfrage

Diese Art der Abfrage wird nur von Linux-basierten Verteilungspunkten unterstützt.

Ein Verteilungspunkt kann Netzwerke abfragen, die Geräte mit IPv6-Adressen enthalten. In diesem Fall werden keine IP-Bereiche angegeben und der Verteilungspunkt fragt das gesamte Netzwerk unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. Um Zeroconf verwenden zu können, müssen Sie das Tool "avahi-browser" auf dem Verteilungspunkt installieren.

So aktivieren Sie die Zeroconf-Abfrage:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **IP-Bereiche**.

   Sie können aus dem Ordner **Nicht zugeordnete Geräte** zum **Gerätesuche** wechseln. Klicken Sie dazu auf **Jetzt abfragen**.

2. Klicken Sie auf die Schaltfläche **Abfrageeinstellungen anpassen**.

3. Wählen Sie in dem sich öffnenden IP-Bereich-Fenster **Abfragen mit Zeroconf-Technologie aktivieren** aus.

Danach beginnt der Verteilungspunkt das Netzwerk abzufragen. In diesem Fall werden die angegeben IP-Bereiche ignoriert.

Arbeit mit Windows-Domänen. Domäneneinstellungen anzeigen und ändern

Um die Einstellungen einer Domäne zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **Domänen**.

2. Wählen Sie eine Domäne aus, und öffnen Sie das Eigenschaftenfenster der Domäne auf eine der folgenden Arten:

   - Wählen Sie **Eigenschaften** im Kontextmenü der Domain.

   - Klicken Sie auf den Link **Gruppeneigenschaften anzeigen**.

<Domänenname> geöffnet, in dem Sie die Einstellungen der gewählten Domäne anpassen können.

Aufbewahrungsregeln für nicht zugeordnete Geräte anpassen

Nach Abschluss der Windows-Netzwerkabfrage werden die gefundenen Geräte in Untergruppen der Administrationsgruppe "Nicht zugeordnete Geräte" zusammengefasst. Diese Administrationsgruppe befindet sich unter **Erweitert** → **Gerätesuche** → **Domänen**. Der Ordner **Domänen** ist die übergeordnete Gruppe. Sie enthält untergeordnete Gruppen, die nach den entsprechenden Domänen und Arbeitsgruppen benannt sind, die bei der Netzwerkabfrage gefunden wurden. Die übergeordnete Gruppe kann auch die Administrationsgruppe für mobile Geräte enthalten. Die Aufbewahrungsregeln für nicht zugeordnete Geräte können für die übergeordnete sowie für jede untergeordnete Gruppe angepasst werden. Die Aufbewahrungsregeln sind nicht von den Einstellungen der Netzwerkabfrage abhängig und sind selbst dann aktiv, wenn die Netzwerkabfrage deaktiviert ist.

Um die Aufbewahrungsregeln für nicht zugeordnete Geräte anzupassen, gehen Sie wie folgt vor:

1. Führen Sie in der Konsolenstruktur im Ordner **Gerätesuche** eine der folgenden Aktionen aus:

   - Um die Einstellungen der übergeordneten Gruppe anzupassen, klicken Sie mit der rechten Maustaste auf den Unterordner **Domänen** und wählen Sie **Eigenschaften** aus.

     Das Eigenschaftenfenster der übergeordneten Gruppe wird geöffnet.

   - Um die Einstellungen einer untergeordneten Gruppe anzupassen, klicken Sie mit der rechten Maustaste auf ihren Namen und wählen Sie **Eigenschaften** aus.

     Das Eigenschaftenfenster der untergeordneten Gruppe wird geöffnet.

2. Geben Sie im Abschnitt **Geräte** die folgenden Einstellungen an:

   - **Gerät aus Gruppe entfernen, wenn Gerät inaktiv seit mehr als (Tagen)**

     Wenn diese Option aktiviert ist, können Sie das Zeitintervall festlegen, nach dem das Geräte automatisch aus der Gruppe gelöscht wird. Standardmäßig wird diese Option auch an die untergeordneten Gruppen weitergegeben. Standardmäßig beträgt das Zeitintervall 7 Tage.

     Diese Option ist standardmäßig aktiviert.

   - **Aus übergeordneter Gruppe erben**

     Wenn diese Option aktiviert ist, wird der Aufbewahrungszeitraum für die Geräte in der aktuellen Gruppe von der übergeordneten Gruppe geerbt und kann nicht geändert werden.

     Diese Option ist nur für untergeordnete Gruppen verfügbar.

     Diese Option ist standardmäßig aktiviert.

   - **Vererben für untergeordnete Gruppen erzwingen**

     Die Einstellungswerte werden an untergeordnete Gruppen verteilt, aber in den Eigenschaften der untergeordneten Gruppen sind diese Einstellungen gesperrt.

     Diese Option ist standardmäßig deaktiviert.

Ihre Änderungen werden gespeichert und übernommen.

Arbeiten mit IP-Bereichen

Sie können die Einstellungen der vorhandenen IP-Bereiche anpassen und neue IP-Bereiche erstellen.

IP-Bereich erstellen

Um einen IP-Bereich zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **IP-Bereiche**.
2. Wählen Sie im Kontextmenü des Ordners **Neu → IP-Bereich** aus.
3. Konfigurieren Sie im folgenden Fenster **Neuer IP-Bereich** die Einstellungen des zu erstellenden IP-Bereichs.

Daraufhin wird der neue IP-Bereich im Ordner **IP-Bereiche** angezeigt.

Einstellungen eines IP-Bereichs anzeigen und ändern

Um die Einstellungen der Abfrage eines IP-Bereichs anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **IP-Bereiche**.
2. Wählen Sie einen IP-Bereich aus, und öffnen Sie sein Eigenschaftenfenster auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf den IP-Bereich, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Gruppeneigenschaften anzeigen**.

<Name des IP-Bereichs> geöffnet, in dem Sie die Einstellungen des gewählten IP-Bereichs anpassen können.

Active Directory Gruppen. Gruppeneinstellungen anzeigen und ändern

Um die Einstellungen einer Gruppe des Active Directory zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **Active Directory**.
2. Wählen Sie die erforderliche Gruppe des Active Directory, und öffnen Sie das Eigenschaftenfenster der Gruppe auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf den IP-Bereich, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Gruppeneigenschaften anzeigen**.

Das wird Fenster **Eigenschaften: <Gruppenname des Active Directory>** geöffnet, in dem Sie die Einstellungen der gewählten Gruppe des Active Directory anpassen können.

Regeln für das automatische Verschieben von Geräten in Administrationsgruppen erstellen

Sie können das automatische Verschieben von Geräten, die während der Abfrage des Firmennetzwerks gefunden werden, in Administrationsgruppen einstellen.

Um die Regeln für das automatische Verschieben von Geräten in Administrationsgruppen festzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Nicht zugeordnete Geräte** aus.
2. Klicken Sie im Arbeitsbereich des Ordners auf die Schaltfläche **Regeln anpassen**.

   Daraufhin wird das Fenster **Eigenschaften: Nicht zugeordnete Geräte** geöffnet. Konfigurieren Sie die Regeln für das automatische Verschieben von Geräten in Administrationsgruppen im Abschnitt **Geräte verschieben**.

Die erste anwendbare Regel in der Liste (von oben nach unten) wird auf ein Gerät angewendet.

Dynamischen VDI-Modus auf Client-Geräten verwenden

Im Netzwerk eines Unternehmens kann eine virtuelle Infrastruktur mit befristeter Nutzung virtueller Maschinen bereitgestellt werden. Kaspersky Security Center erkennt temporäre virtuelle Maschinen und fügt ihre Daten zur Administrationsserver-Datenbank hinzu. Nachdem der Benutzer seine Arbeit auf der temporären virtuellen Maschine beendet hat, wird die virtuelle Maschine aus der virtuellen Infrastruktur entfernt. Der Eintrag der virtuellen Maschine kann jedoch in der Datenbank des Administrationsservers gespeichert werden. Darüber hinaus können nicht vorhandene virtuelle Maschinen in der Verwaltungskonsole angezeigt werden.

Damit keine Daten über nicht vorhandene virtuelle Maschinen gespeichert werden, wurde in Kaspersky Security Center die Unterstützung des dynamischen Modus für die Virtual Desktop Infrastructure (VDI) realisiert. Der Administrator kann die Unterstützung des dynamischen Modus für VDI in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren, das auf einer temporären virtuellen Maschine installiert wird.

Wird die temporäre virtuelle Maschine heruntergefahren, informiert der Administrationsagent darüber den Administrationsserver. Wurde die virtuelle Maschine erfolgreich heruntergefahren, wird sie aus der Liste der Geräte entfernt, die mit dem Administrationsserver verbunden sind. Wurde die virtuelle Maschine fehlerhaft heruntergefahren, und der Administrationsagent hat keine Benachrichtigung darüber an den Administrationsserver gesendet, wird eine Backup-Szenario angewendet. In diesem Fall wird die virtuelle Maschine nach drei fehlgeschlagenen Synchronisierungsversuchen mit dem Server aus der Liste der mit dem Administrationsserver verbundenen Geräte entfernt.

Dynamischen VDI-Modus in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren

Gehen Sie wie folgt vor, um den dynamischen VDI-Modus zu aktivieren:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.
2. Klicken Sie mit der rechten Maustaste auf das Installationspaket des Administrationsagenten und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: Kaspersky Security Center Administrationsagent** wird geöffnet.
3. Wählen Sie im Fenster **Eigenschaften: Kaspersky Security Center Administrationsagent** den Abschnitt **Erweitert** aus.
4. Aktivieren Sie auf der Registerkarte **Erweitert** die Option **Dynamischen Modus für VDI aktivieren**.

Das Gerät, auf dem der Administrationsagent installiert wird, wird in die VDI aufgenommen.

Geräte suchen, die zu VDI gehören

Gehen Sie wie folgt vor, um nicht zugeordnete Geräte zu finden, die zu VDI gehören:

1. Klicken Sie mit der rechten Maustaste auf den Ordner **Nicht zugeordnete Geräte** und wählen Sie **Suchen** aus.

   Um eine Liste aller Geräte anzuzeigen, die Teil der Virtual Desktop Infrastructure sind, wählen Sie im Kontextmenü des Ordners **Administrationsserver** die Option **Suchen**.
2. Wählen Sie im Fenster **Suchen** auf der Registerkarte **Virtuelle Maschinen** in der Einstellungsgruppe **Teil einer Virtual Desktop Infrastructure (VDI)** die Option **Ja** aus.
3. Klicken Sie auf die Schaltfläche **Suchen**.

Die Liste der nicht zugewiesenen Geräte, die Teil der Virtual Desktop Infrastructure sind, wird angezeigt.

Geräte, die zu VDI gehören, in eine Administrationsgruppe verschieben

Gehen Sie wie folgt vor, um Geräte, die zur VDI gehören, in eine Administrationsgruppe zu verschieben:

1. Klicken Sie im Arbeitsbereich des Ordners **Nicht zugeordnete Geräte** auf **Regeln anpassen**.

   Daraufhin wird das Eigenschaftenfenster des Ordners **Nicht zugeordnete Geräte** geöffnet.
2. Klicken Sie im Eigenschaftenfenster des Ordners **Nicht zugeordnete Geräte** im Abschnitt **Geräte verschieben** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Neue Regel** wird geöffnet.
3. Wählen Sie im Fenster **Neue Regel** den Abschnitt **Virtuelle Maschinen** aus.
4. Wählen Sie in der Dropdown-Liste **Dies ist eine virtuelle Maschine** die Option **Ja**.

Daraufhin wird eine Regel für das Verschieben von Geräten in eine Administrationsgruppe erstellt.

Arbeitsgerätebestand

Die Hardware-Liste (**Datenverwaltung** → **Hardware**), die Sie für die Inventur der Arbeitsgeräte verwenden, wird auf zwei Arten gefüllt: automatisch und manuell. Nach jeder Netzwerkabfrage werden alle erkannten Geräte automatisch in die Liste eingetragen. Sie können Geräte aber auch manuell hinzufügen, wenn Sie das Netzwerk nicht abfragen möchten. Sie können manuell weitere Geräte zu der Liste hinzufügen, z. B. Router, Drucker und andere Geräte-Hardware.

In den Eigenschaften eines Geräts können Sie sich ausführliche Informationen über das Gerät anzeigen lassen und diese bearbeiten.

Die Hardware-Liste kann die folgenden Gerätetypen enthalten:

- Computer
- Mobile Geräte
- Netzwerkgeräte
- virtuelle Geräte
- Computer-Hardware (OEM)
- Computer-Peripheriegeräte
- angeschlossene Geräte
- VoIP-Telefonie
- Netzwerkspeicher

Der Administrator kann den gefundenen Geräten das Merkmal *Für Unternehmen* zuweisen. Er kann dieses Merkmal in den Eigenschaften des Geräts manuell zuweisen oder die Kriterien für die automatische Zuweisung festlegen. In diesem Fall wird das Merkmal *Für Unternehmen* nach dem Typ des Geräts zugewiesen.

Kaspersky Security Center ermöglicht es, eine Abschreibung von Hardware durchzuführen. Aktivieren Sie dazu in den Eigenschaften des Geräts die Option **Das Gerät wurde abgeschrieben**. Ein solches Gerät wird in der Hardware-Liste nicht angezeigt.

Der Administrator kann im Ordner **Hardware** die Liste der speicherprogrammierbaren Steuerungen (SPS) verwenden. Ausführliche Informationen zur Verwendung von SPS-Listen finden Sie im *Benutzerhandbuch für Kaspersky Industrial CyberSecurity for Nodes*.

Informationen über neue Geräte hinzufügen

Um Informationen über neue Geräte hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Datenverwaltung** der Konsolenstruktur den Unterordner **Hardware** aus.
2. Öffnen Sie durch Klicken auf die Schaltfläche **Gerät hinzufügen** im Arbeitsbereich des Ordners **Hardware** das Fenster **Neues Gerät**.

   Das Fenster **Neues Gerät** wird geöffnet.
3. Wählen Sie im Fenster **Neues Gerät** in der Dropdown-Liste **Typ** den Typ des Gerätes aus, das Sie hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **OK**.

   Das Fenster mit den Geräte-Eigenschaften im Abschnitt **Allgemein** wird geöffnet.
5. Füllen Sie im Abschnitt **Allgemein** die Eingabefelder mit den Daten über das Gerät aus. Im Abschnitt **Allgemein** werden die folgenden Einstellungen angezeigt:

   - **Unternehmensgerät**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie dem Gerät das Merkmal *Für Unternehmen* zuweisen möchten. Nach diesem Merkmal können Sie Suche nach Geräten im Ordner **Hardware** durchführen.
   - **Das Gerät wurde abgeschrieben**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass das Gerät in der Geräteliste im Ordner **Hardware** angezeigt wird.
6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Das neue Gerät wird im Arbeitsbereich des Ordners **Hardware** angezeigt.

Kriterien zur Erkennung von Unternehmensgeräten anpassen

Um Kriterien zur Erkennung von Unternehmensgeräten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Datenverwaltung** der Konsolenstruktur den Unterordner **Hardware** aus.
2. Klicken Sie im Arbeitsbereich des Ordners **Hardware** auf die Schaltfläche **Weitere Aktionen** und wählen Sie in der Dropdown-Liste die Option **Regel für Geräte mit Merkmal "Unternehmensgerät" einrichten**.

   Das Eigenschaftenfenster der Hardware wird geöffnet.

3. Wählen Sie im Hardware-Eigenschaftenfenster im Abschnitt **Unternehmensgeräte** eine Methode für die Zuweisung des Merkmals *Für Unternehmen* zum Gerät aus:

   - **Merkmal "Unternehmensgerät" für das Gerät manuell setzen**. Das Merkmal *Für Unternehmen* wird dem Gerät manuell im Eigenschaftenfenster des Geräts im Abschnitt **Allgemein** zugewiesen.

   - **Merkmal "Unternehmensgerät" für das Gerät automatisch setzen**. Geben Sie in der Einstellungsgruppe **Nach dem Gerätetyp** die Gerätetypen an, denen das Programm das Merkmal *Für Unternehmen* automatisch zuweisen soll.

     Diese Option wirkt sich nur auf die Geräte aus, die durch Netzwerkabfrage hinzugefügt wurden. Stellen Sie für die manuell hinzugefügten Geräte das Merkmal *Für Unternehmen* manuell ein.

4. Klicken Sie auf die Schaltfläche **OK**.

Die Kriterien zur Bestimmung von Unternehmensgeräte sind konfiguriert.

Benutzerdefinierte Felder anpassen

Um die benutzerdefinierten Felder der Geräte anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Datenverwaltung** der Konsolenstruktur den Unterordner **Hardware** aus.

2. Klicken Sie im Arbeitsbereich des Ordners **Hardware** auf die Schaltfläche **Weitere Aktionen** und wählen Sie in der Dropdown-Liste die Option **Benutzerdefinierte Datenfelder anpassen**.

   Das Eigenschaftenfenster der Hardware wird geöffnet.

3. Klicken Sie im Eigenschaftenfenster der Hardware im Abschnitt **Benutzerdefinierte Felder** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Feld hinzufügen** wird geöffnet.

4. Geben Sie im Fenster **Feld hinzufügen** den Namen des benutzerdefinierten Feldes an, das in den Eigenschaften der Hardware angezeigt werden soll.

   Sie können mehrere benutzerdefinierte Felder mit eindeutigen Namen erstellen.

5. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin werden in den Eigenschaften der Hardware im Abschnitt **Benutzerdefinierte Felder** die hinzugefügten benutzerdefinierten Felder angezeigt. Sie können die benutzerdefinierte Felder verwenden, um spezifische Informationen zu den Geräten anzugeben. Dazu gehört z. B. die innerbetriebliche Bestellnummer für die Hardware.

Lizenzierung

Dieser Abschnitt informiert über die grundlegenden Konzepte, die mit der Lizenzierung von Kaspersky Security Center 15.1 zusammenhängen.

Ereignisse bei Überschreitung der Lizenzbeschränkung

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über Ereignisse der Überschreitung der Lizenzbeschränkung von Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind.

Die Ereigniskategorie für die Überschreitung der Lizenzbeschränkung wird anhand folgender Regeln bestimmt:

- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz zwischen 90% und 100% der Gesamtmenge der Lizenzeinheiten dieser Lizenz liegt, wird das Ereignis in der Ereigniskategorie **Infomeldung** veröffentlicht.
- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz zwischen 100% und 110% der Gesamtmenge der Lizenzeinheiten dieser Lizenz liegt, wird das Ereignis in der Ereigniskategorie **Warnung** veröffentlicht.
- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz 110% der Gesamtmenge der Lizenzeinheiten dieser Lizenz übersteigt, wird das Ereignis in der Ereigniskategorie **Kritisches Ereignis** veröffentlicht.

Über die Lizenzierung

Dieser Abschnitt enthält Informationen über die Lizenzierung von Kaspersky-Anwendungen, die mittels Kaspersky Security Center verwaltet werden.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für Kaspersky Security Center, das Ihnen gemäß den Bedingungen des unterzeichneten Lizenzvertrags (Endbenutzer-Lizenzvertrag) überlassen wird.

Der Umfang der Leistungen und die Laufzeit hängen vom Typ der Lizenz ab, mit der das Programm verwendet wird.

Es sind folgende Lizenztypen vorgesehen:

- *Test*

  Eine kostenlose Lizenz zum Kennenlernen der Anwendung. Eine Testlizenz verfügt in der Regel über eine kurze Gültigkeitsdauer.

  Nachdem die Gültigkeit einer Demolizenz abgelaufen ist, stellt Kaspersky Security Center die Funktion ein. Um das Programm weiter nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

  Die Anwendung kann nur einmal im Rahmen einer Demolizenz verwendet werden.

- *Kommerziell*

  Eine kostenpflichtige Lizenz.

  Wenn eine kommerzielle Lizenz abläuft, werden wichtige Anwendungsfunktionen deaktiviert. Zur weiteren Nutzung von Kaspersky Security Center ist eine Verlängerung der kommerziellen Lizenz erforderlich. Nach Ablauf einer kommerziellen Lizenz können Sie die Anwendung nicht mehr verwenden und müssen es von Ihrem Gerät entfernen.

  Es wird empfohlen, die Gültigkeitsdauer Ihrer Lizenz vor deren Ablaufdatum zu verlängern, um einen ununterbrochenen Schutz vor allen Sicherheitsbedrohungen zu gewährleisten.

Über den Endbenutzer-Lizenzvertrag

Der *Endbenutzer-Lizenzvertrag* (Lizenzvertrag oder EULA) ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie sich den Lizenzvertrag bitte sorgfältig durch, bevor Sie die Anwendung nutzen.

Kaspersky Security Center und die einzelnen Komponenten (z. B. Administrationsagent) haben jeweils eine eigene EULA.

Sie können die Bedingungen des Endbenutzer-Lizenzvertrags für Kaspersky Security Center wie folgt anzeigen:

- Während der Installation von Kaspersky Security Center.
- Mithilfe des Dokuments license.txt, das zum Lieferumfang von Kaspersky Security Center gehört.
- Mithilfe des Dokuments license.txt im Installationsordner von Kaspersky Security Center.
- Durch Herunterladen der Datei license.txt von der Website von Kaspersky.

Sie können die Bedingungen der Endbenutzer-Lizenzverträge für die Administrationsagenten für Windows, Mac und Linux wie folgt anzeigen:

- Während das Programmpaket für den Administrationsagenten von den Kaspersky-Webservern heruntergeladen wird.
- Während der Installation eines Administrationsagenten für Windows, Mac oder Linux.
- In dem Dokument license.txt, welches im Programmpaket der Administrationsagenten für Windows, Mac und Linux enthalten ist.
- In dem Dokument license.txt, welches im Installationsordner der Administrationsagenten für Windows, Mac und Linux enthalten ist.
- Durch Herunterladen der Datei license.txt von der Website von Kaspersky.

Wenn Sie bei der Anwendungsinstallation dem Text des Endbenutzer-Lizenzvertrags zustimmen, gelten die Bedingungen des Endbenutzer-Lizenzvertrags als akzeptiert. Falls Sie den Lizenzvertrag ablehnen, brechen Sie die Anwendungsinstallation ab und nutzen Sie die Anwendung nicht.

Über das Lizenzzertifikat

Ein *Lizenzzertifikat* ist ein Dokument, das Ihnen zusammen mit einer Schlüsseldatei bzw. einem Aktivierungscode übergeben wird.

Das Lizenzzertifikat enthält folgende Informationen über die ausgestellte Lizenz:

- Lizenz-ID oder Bestellnummer
- Informationen über den Benutzer, dem die Lizenz ausgestellt wird

- Informationen über die Anwendung, das mit der ausgestellten Lizenz aktiviert werden kann
- Maximale Anzahl von Lizenzeinheiten (z. B. Geräte, auf denen die Anwendung unter dieser Lizenz verwendet werden kann)
- Datum für den Beginn der Lizenzgültigkeit
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über den Lizenzschlüssel

Ein *Lizenzschlüssel* ist eine Bitsequenz, mit deren Hilfe Sie die Anwendung aktivieren können, um diese dann in Übereinstimmung mit dem Endbenutzer-Lizenzvertrag zu nutzen. Der Lizenzschlüssel wird von den Experten von Kaspersky generiert.

Sie können einen Lizenzschlüssel mithilfe einer der folgenden Methoden zur Anwendung hinzufügen: durch Anwendung einer *Schlüsseldatei* oder Eingabe eines *Aktivierungscodes*. Nachdem Sie den Lizenzschlüssel in der Anwendung hinzugefügt haben, wird er in der Programmoberfläche als eindeutige Folge aus Buchstaben und Ziffern angezeigt.

Ein Lizenzschlüssel kann von Kaspersky gesperrt werden, falls die Bedingungen des Lizenzvertrags verletzt wurden. Wenn ein Lizenzschlüssel gesperrt wurde, muss ein anderer Schlüssel hinzugefügt werden, um die Anwendung zu nutzen.

Ein Lizenzschlüssel kann entweder aktiv oder zusätzlich (Reserve) sein.

Ein *aktiver Lizenzschlüssel* ist ein Lizenzschlüssel, der momentan von der Anwendung verwendet wird. Ein aktiver Lizenzschlüssel kann für eine Test- oder kommerzielle Lizenz hinzugefügt werden. In der Anwendung kann jeweils nur ein aktiver Lizenzschlüssel vorhanden sein.

Ein *zusätzlicher (oder Reserve-) Lizenzschlüssel* ist ein Lizenzschlüssel, der das Recht auf Nutzung der Anwendung bestätigt, jedoch im Augenblick nicht verwendet wird. Der Reserve-Lizenzschlüssel wird automatisch aktiviert, wenn die Gültigkeitsdauer der Lizenz abläuft, die zum aktiven Lizenzschlüssel gehört. Ein Reserve-Lizenzschlüssel kann nur hinzugefügt werden, wenn ein aktiver Lizenzschlüssel vorhanden ist.

Der Lizenzschlüssel für eine Demolizenz kann als aktiver Lizenzschlüssel hinzugefügt werden. Der Lizenzschlüssel für eine Demolizenz kann nicht als Reserve-Lizenzschlüssel hinzugefügt werden.

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Schlüsseldateien dienen zum Aktivieren der Anwendung durch Hinzufügen eines Lizenzschlüssels.

Sie erhalten eine Schlüsseldatei an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center oder bei der Anforderung der Testversion von Kaspersky Security Center angegeben haben.

Um die Anwendung mithilfe der Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Kaspersky-Aktivierungsservern erforderlich.

Wenn die Schlüsseldatei versehentlich gelöscht wurde, können Sie diese wiederherstellen. Eine Schlüsseldatei kann beispielsweise für die Registrierung eines Kaspersky CompanyAccount erforderlich sein.

Um Ihre Schlüsseldatei wiederherzustellen, führen Sie eine der folgenden Aktionen aus:

- Wenden Sie sich an den Lizenzverkäufer.
- Schlüsseldatei anhand eines vorhandenen Aktivierungscodes auf der Website von Kaspersky abrufen.
- Exportieren Sie eine Lizenzschlüsseldatei von einem anderen Administrationsserver.

Über das Abonnement

Ein *Abonnement für Kaspersky Security Center* ist eine Bestellung des Programms mit bestimmten Einstellungen (Ablaufdatum des Abonnements, Anzahl der geschützten Geräte). Ein Abonnement für Kaspersky Security Center kann bei einem Lieferanten von Dienstleistungen abgeschlossen werden (z. B. bei einem Internet-Provider). Das Abonnement kann manuell oder automatisch verlängert oder auch gekündigt werden.

Ein Abonnement kann beschränkt (z. B. auf ein Jahr) oder unbeschränkt (ohne Ablaufdatum) sein. Um Kaspersky Security Center weiterhin zu nutzen, muss ein beschränktes Abonnement rechtzeitig verlängert werden. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Dienstleister überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abonnement-Verlängerung gewährt, innerhalb dieser die Funktionalität der Anwendung erhalten bleibt. Verfügbarkeit und Dauer der Nachfrist werden vom Lieferanten der Dienstleistungen bestimmt.

Um Kaspersky Security Center mit einem Abonnement zu nutzen, muss der Aktivierungscode übernommen werden, den Sie von Ihrem Provider erhalten.

Sie können nur dann einen anderen Aktivierungscode für die Nutzung von Kaspersky Security Center verwenden, wenn das Abonnement zuvor abgelaufen ist oder gekündigt wurde.

Für die Abonnement-Verwaltung stehen je nach Provider unterschiedliche Optionen zur Verfügung. Der Provider stellt möglicherweise keine Nachfrist für die Verlängerung des Abonnements zur Verfügung, innerhalb der die Funktionen der Anwendung erhalten bleiben.

Die für ein Abonnement erhaltenen Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Security Center verwendet werden.

Bei einer Nutzung des Programms im Abonnement stellt Kaspersky Security Center zum festgelegten Zeitpunkt vor Ablauf des Abonnements automatisch eine Verbindung zum Aktivierungsserver her. Dadurch wird sichergestellt, dass die Informationen über das Abonnement mit dem Aktivierungsserver synchronisiert werden. Wenn der Zugriff auf den Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung öffentliche DNS-Server. Sie können das Abonnement auf der Website des Providers verlängern.

Sie können die Informationen über das Abonnement manuell aktualisieren, ohne abzuwarten, dass Kaspersky Security Center auf den Aktivierungsserver zugreift. Dies kann nützlich sein, wenn Sie die Abonnementeinstellungen ändern.

So aktualisieren Sie die Informationen über das Abonnement manuell:

1. Wählen Sie in der Konsolenstruktur den Ordner **Lizenzen für Kaspersky-Software** aus.
2. Klicken Sie auf **Weitere Aktionen** und wählen Sie in der Dropdown-Liste den Punkt **Abonnement-Einstellungen mit dem Lizenzserver synchronisieren** aus.

Die Informationen über das Abonnement werden auf dem Aktivierungsserver aktualisiert.

Über den Aktivierungscode

Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus 20 Buchstaben und Ziffern. Den Aktivierungscode geben Sie ein, um einen Lizenzschlüssel zur Aktivierung von Kaspersky Security Center hinzuzufügen. Sie erhalten den Aktivierungscode an die von Ihnen angegebene E-Mail-Adresse, nachdem Sie Kaspersky Security Center erworben haben oder eine Testversion von Kaspersky Security Center bestellt haben.

Um das Programm unter Verwendung eines Aktivierungscodes zu aktivieren, ist ein Internetzugang für die Verbindung mit den Aktivierungsservern von Kaspersky erforderlich. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server.

Wenn das Programm mithilfe eines Aktivierungscodes aktiviert wurde, sendet das Programm in einigen Fällen nach der Aktivierung regelmäßige Anfragen an die Aktivierungsserver von Kaspersky zur Überprüfung des aktuellen Lizenzschlüsselstatus. Zum Versenden von Anfragen benötigt das Programm einen Internetzugang.

Wenn Sie Ihren Aktivierungscode nach der Installation des Programms verloren haben, wenden Sie sich an den Kaspersky-Partner, von dem Sie die Lizenz erworben haben.

Sie können keine Schlüsseldateien zum Aktivieren verwalteter Programme verwenden. Es werden nur Aktivierungscodes akzeptiert.

Vereinbarung mit einem Endbenutzer-Lizenzvertrag widerrufen

Wenn Sie den Schutz Ihrer Client-Geräte beenden möchten, können Sie verwaltete Kaspersky-Anwendungen deinstallieren und Ihren Endbenutzer-Lizenzvertrag (EULA) für diese Anwendungen widerrufen.

So widerrufen Sie eine EULA für verwaltete Kaspersky-Anwendungen:

1. Wählen Sie in der Konsolenstruktur **Administrationsserver** → **Erweitert** → **Akzeptierte EULAs** aus.

   Es wird eine Liste der EULAs angezeigt, die beim Erstellen von Installationspaketen, bei der nahtlosen Installation von Updates oder bei der Bereitstellung von Kaspersky Security für mobile Endgeräte akzeptiert wurden.

2. Wählen Sie in der Liste die EULA aus, die Sie widerrufen möchten.

   Sie können die folgenden Eigenschaften der EULA anzeigen:

   - Datum, an dem die EULA akzeptiert wurde.
   - Name des Benutzers, der die EULA akzeptiert hat.
   - Link zu den Bedingungen der EULA.
   - Liste der Objekte, die mit der EULA verbunden sind: Namen der Installationspakete, Namen nahtloser Updates, Namen mobiler Anwendungen.

3. Klicken Sie auf die Schaltfläche **EULA widerrufen**.

   In dem sich öffnenden Fenster werden Sie darüber informiert, dass Sie die Kaspersky-Anwendung deinstallieren müssen, welches dieser EULA entspricht.

4. Klicken Sie auf die Schaltfläche, um den Widerruf zu bestätigen.

   Kaspersky Security Center prüft, ob die Installationspakete (die der verwalteten Kaspersky-Anwendung entsprechen, deren EULA Sie widerrufen möchten) gelöscht wurden.

   Sie können die EULA nur für eine verwaltete Kaspersky-Anwendung widerrufen, dessen Installationspakete gelöscht werden.

Die EULA wurde widerrufen. Sie wird nicht in der Liste der EULAs im Abschnitt **Administrationsserver → Erweitert → Akzeptierte EULAs** angezeigt. Sie können Client-Geräte nicht durch eine Kaspersky-Anwendung schützen, deren EULA Sie widerrufen haben.

Über die Bereitstellung von Daten

An Dritte übertragene Daten

Wenn Sie die Software-Funktionalität "Verwaltung mobiler Geräte" verwenden, wird der Cloud-Messaging-Dienst Google Firebase verwendet, um Befehle über den Push-Benachrichtigungsmechanismus rechtzeitig an Geräte zu senden, auf denen das Android-Betriebssystem ausgeführt wird. Wenn der Benutzer die Nutzung des Cloud-Messaging-Dienstes Google Firebase konfiguriert hat, erklärt er sich damit einverstanden, dem Google Firebase Cloud-Messaging-Dienst die folgenden Informationen im automatischen Modus bereitzustellen: Installations-IDs der Programme von Kaspersky Endpoint Security für Android, an welche Push-Benachrichtigungen gesendet werden müssen.

Um den Informationsaustausch mit dem Google Firebase Cloud-Messaging-Dienst zu blockieren, muss der Benutzer die Einstellungen des Google Firebase Cloud-Messaging-Dienstes zurücksetzen.

Wenn Sie Software-Funktionalität "Verwaltung mobiler Geräte" verwenden, wird zur rechtzeitigen Übermittlung von Befehlen mittels Push-Benachrichtigungsmechanismus an Geräte, auf denen das iOS-Betriebssystem ausgeführt wird, der Apple Push Notification Service (APNS) verwendet. Wenn der Benutzer ein APNs-Zertifikat auf einem iOS MDM-Server installiert hat, ein iOS MDM-Profil mit einer Reihe von Einstellungen für die Verbindung von mobilen iOS-Geräten mit der Software erstellt, und wenn er dieses iOS MDM-Profil auf mobilen Geräten installiert, erklärt er sich damit einverstanden, die folgenden Informationen an APNs im automatischen Modus bereitzustellen:

- Token – Push-Token des Geräts. Der Server verwendet diesen Token beim Senden von Push-Benachrichtigungen an das Gerät.
- PushMagic – Zeichenfolge, die in der Push-Benachrichtigung enthalten sein muss. Der Wert dieser Zeichenfolge wird vom Gerät generiert.

Lokal verarbeitete Daten

Das Programm Kaspersky Security Center dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentral zu erledigen. Kaspersky Security Center ermöglicht es dem Administrator, auf detaillierte Informationen über die Sicherheitsstufe des Unternehmensnetzwerks zuzugreifen und alle Schutzkomponenten zu konfigurieren, die auf Kaspersky-Anwendungen basieren. Die folgenden Hauptfunktionen werden von Kaspersky Security Center ausgeführt:

- Erkennen von Geräten und deren Benutzern im Unternehmensnetzwerk
- Erstellen einer Hierarchie von Administrierungsgruppen für die Geräteverwaltung
- Installieren von Kaspersky-Anwendungen auf Geräten

- Verwalten der Einstellungen und Aufgaben von installierten Programmen
- Verwalten der Updates für Kaspersky- und Drittanbieter-Anwendungen sowie Auffinden und Schließen von Schwachstellen
- Aktivieren von Kaspersky-Anwendungen auf Geräten
- Verwalten von Benutzerkonten
- Anzeigen von Informationen zur Ausführung von Kaspersky-Anwendungen auf Geräten
- Anzeigen von Berichten

Um seine Hauptfunktionen auszuführen, kann Kaspersky Security Center die folgenden Informationen empfangen, speichern und verarbeiten:

- Informationen über die Geräte im Unternehmensnetzwerk, die durch das Scannen der Windows-Domäne, der Active Directory- oder Samba-Domänencontroller oder durch das Scannen von IP-Bereichen erhalten wurden. Der Administrationsserver bezieht die Daten entweder selbstständig oder erhält sie von einem Administrationsagenten, der als Verteilungspunkt fungiert.
- Informationen aus Active Directory und Samba über Organisationseinheiten, Domänen, Benutzer und Gruppen. Der Administrationsserver bezieht die Daten entweder selbstständig oder erhält sie von einem Administrationsagenten, der als Verteilungspunkt fungiert.
- Einzelheiten zu den verwalteten Geräten Der Administrationsagent übermittelt die unten aufgeführten Daten von dem Gerät an den Administrationsserver. Der Benutzer gibt den Anzeigenamen und die Beschreibung des Geräts in der Benutzeroberfläche der Verwaltungskonsole oder in der Benutzeroberfläche von Kaspersky Security Center Web Console ein:
  - Technische Spezifikationen des verwalteten Geräts und seiner Komponenten, die zur Geräteidentifizierung erforderlich sind: Anzeigename und Beschreibung des Geräts, Typ und Name der Windows-Domäne, Gerätename in der Windows-Umgebung, DNS-Domäne und DNS-Name, IPv4-Adresse, IPv6-Adresse, Netzwerkadresse, MAC-Adresse, Seriennummer, Betriebssystemtyp, ob das Gerät eine virtuelle Maschine mit Hypervisor-Typ ist oder ob das Gerät eine dynamische virtuelle Maschine als Teil von VDI ist.
  - Weitere Spezifikationen verwalteter Geräte und ihrer Komponenten, die für die Prüfung verwalteter Geräte und für die Entscheidung, ob bestimmte Patches und Updates anwendbar sind, erforderlich sind: Status von Windows Update-Agent (WUA); Architektur des Betriebssystems; Hersteller des Betriebssystems; Versionsnummer des Betriebssystems; Release-ID des Betriebssystems; Speicherort des Betriebssystems; wenn das Gerät eine virtuelle Maschine ist: Typ der virtuellen Maschine; Name des virtuellen Administrationsservers, der das Gerät verwaltet; Daten des Cloud-Geräts (Cloud-Region, VPC, Availability Zone (Verfügbarkeitszone) der Cloud, Subnetz der Cloud).
  - Details zu Aktionen auf verwalteten Geräten: Datum und Uhrzeit des letzten Updates; Uhrzeit, zu der das Gerät zuletzt im Netzwerk sichtbar war; Neustart-Wartestatus; Uhrzeit, zu der das Gerät eingeschaltet wurde.
  - Details zu Gerätebenutzerkonten und den deren Arbeitssitzungen.
- Daten, die beim Ausführen der Ferndiagnose auf einem verwalteten Gerät empfangen werden: Ablaufverfolgungsdateien, Systeminformationen, Details zu den auf dem Gerät installierten Kaspersky-Anwendungen, Dump-Dateien, Ereignisprotokolle, Ausführungsergebnisse der vom Kaspersky Technischen Support bereitgestellten Diagnoseskripte.
- Statistiken zum Verteilungspunkt-Betrieb, wenn das Gerät ein Verteilungspunkt ist. Der Administrationsagent übermittelt Daten von dem Gerät an den Administrationsserver.

- Vom Benutzer in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console eingegebene Einstellungen für Verteilungspunkte.

- Daten, die für die Verbindung von mobilen Geräten mir dem Administrationsserver notwendig sind: Zertifikat, Port der mobilen Verbindung, Verbindungsadresse des Administrationsservers. Der Benutzer gibt Daten in die Verwaltungskonsole oder in Kaspersky Security Center Web Console ein.

- Details zu mobilen Geräten, die mit dem iOS MDM-Protokoll übertragen werden. Die unten aufgelisteten Daten werden vom mobilen Gerät an den Administrationsserver übertragen:

    - Technische Spezifikationen des mobilen Geräts und seiner Komponenten, die zur Geräteidentifizierung erforderlich sind: Gerätename, Modell, Betriebssystemname, Build-Nummer des Betriebssystems, Gerätemodellnummer, IMEI-Nummer, UDID, MEID, Seriennummer, Speichergröße, Modem-Firmware-Version, Bluetooth-MAC-Adresse, Wi-Fi-MAC-Adresse und SIM-Karten-Details (ICCID als Teil der SIM-Karten-ID).

    - Details des vom verwalteten Gerät verwendeten Mobilfunknetzes: Mobilfunknetztyp, Name des derzeit verwendeten Mobilfunknetzes, Name des Heim-Mobilfunknetzes, Version der Mobilfunknetzbetreibereinstellungen, Sprach-Roaming- und Daten-Roaming-Status, Ländercode des Mobilfunknetzes Heimnetzwerk, Ländercode des Wohnsitzes, Code des aktuell verwendeten Netzwerks und Verschlüsselungsgrad.

    - Sicherheitseinstellungen des mobilen Geräts: Verwendung eines Kennworts und seiner Übereinstimmung mit den Richtlinieneinstellungen, Liste der Konfigurationsprofile und Provisioning-Profile für die Installation von Anwendungen von Drittanbietern.

    - Datum der letzten Synchronisation mit dem Administrationsserver und Status der Geräteverwaltung.

- Einzelheiten zu den auf dem Gerät installierten Anwendungen von Kaspersky. Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver:

    - Einstellungen der auf dem verwalteten Gerät installierten Kaspersky-Anwendungen: Name und Version der Kaspersky-Anwendung, Status, Echtzeitschutzstatus, Datum und Uhrzeit der letzten Untersuchung des Geräts, Anzahl der erkannten Bedrohungen, Anzahl der Objekte, deren Desinfektion fehlgeschlagen ist, Verfügbarkeit und Status der Anwendungskomponenten, Zeitpunkt des letzten Updates und Version der Antiviren-Datenbanken, Details zu den Einstellungen und Aufgaben von Kaspersky-Anwendungen, Informationen zu aktiven und Reserve-Lizenzschlüsseln, Installationsdatum der Anwendung und ID.

    - Statistiken zur Anwendungsoperation: Ereignisse im Zusammenhang mit Statusveränderungen von Komponenten der Kaspersky-Anwendungen auf dem verwalteten Gerät und im Zusammenhang mit der Ausführung von Aufgaben, die von den Softwarekomponenten ausgelöst werden.

    - Der Status des Geräts wird von der Kaspersky-Anwendung bestimmt.

    - Von der Kaspersky-Anwendung zugewiesene Tags.

    - Eine Reihe installierter und anwendbarer Updates für die Kaspersky-Anwendung.

- In Ereignissen von Komponenten des Kaspersky Security Centers und von durch Kaspersky verwalteten Programmen enthaltene Daten. Der Administrationsagent übermittelt Daten von dem Gerät an den Administrationsserver.

- Daten, die zur Integration von Kaspersky Security Center in ein SIEM-System für den Ereignisexport erforderlich sind. Der Benutzer gibt Daten in die Verwaltungskonsole oder in Kaspersky Security Center Web Console ein.

- Einstellungen von Komponenten des Kaspersky Security Centers und von durch Kaspersky verwalteten Programmen, die in Richtlinien und Richtlinienprofilen dargestellt werden. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- Aufgabeneinstellungen von Komponenten des Kaspersky Security Centers und von durch Kaspersky verwalteten Programmen. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- Von der Funktion "Schwachstellen- und Patch-Management" verarbeitete Daten. Der Administrationsagent übermittelt die unten aufgeführten Daten von dem Gerät an den Administrationsserver:

  - Einzelheiten zu auf verwalteten Geräten installierten Anwendungen und Patches (Programm-Registry).

  - Informationen über erkannte Hardware auf verwalteten Geräten (Hardware-Register).

    Wenn der Administrationsagent auf einem Windows-Gerät installiert ist, sendet er nur die folgenden Informationen über die Gerätehardware an den Administrationsserver:

    - Arbeitsspeicher
    - Massenspeichergeräte
    - Mainboard
    - Prozessor
    - Netzwerkadapter
    - Monitore
    - Grafikkarte
    - Soundkarte

    Wenn der Administrationsagent auf einem Linux- oder macOS-Gerät installiert ist, sendet er die folgenden Informationen über die Gerätehardware an den Administrationsserver (vorausgesetzt, diese Information wird durch das Betriebssystem bereitgestellt):

    - Gesamtgröße des Arbeitsspeichers
    - Gesamtgröße der Massenspeicher
    - Mainboard
    - Prozessor
    - Netzwerkadapter

  - Details über Schwachstellen in Drittanbieter-Software, die auf verwalteten Geräten gefunden wurden.

  - Details über verfügbare Updates für Drittanbieter-Anwendungen, die auf verwalteten Geräten installiert sind.

- Details über Microsoft-Updates, die von der WSUS-Funktion gefunden wurden.
- Liste der Microsoft-Updates, die von der WSUS-Funktion gefunden wurden und die auf dem Gerät installiert werden müssen.

- Erforderliche Daten zum Herunterladen von Updates auf einen isolierten Administrationsserver, um Schwachstellen in Programmen von Drittanbietern auf verwalteten Geräten zu schließen. Mittels des Administrationsservers-Tools "klscflag" gibt der Benutzer Daten ein und überträgt diese.
- Daten, die für die Zusammenarbeit von Kaspersky Security Center mit den Cloud-Umgebungen (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud) erforderlich sind. Der Benutzer gibt Daten in die Verwaltungskonsole oder in Kaspersky Security Center Web Console ein.
- Benutzerkategorien der Anwendungen. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.
- Informationen über ausführbaren Dateien, die auf verwalteten Geräten durch die Komponente "Programmkontrolle" gefunden werden. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.
- Details zu Dateien, die ins Backup verschoben wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.
- Details zu Dateien, die in die Quarantäne verschoben wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.
- Informationen zu Dateien, die von Kaspersky-Spezialisten für eine detaillierte Analyse angefordert wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.
- Details zum Status und Auslösen von Regeln zur Adaptiven Kontrolle von Anomalien. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.
- Informationen über externe Geräte (Speichereinheiten, Tools zum Informationstransfer, Hardcopy-Tools und Verbindungsbusse), die auf dem verwalteten Gerät installiert oder damit verbunden sind und von der Gerätekontrolle erkannt werden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.
- Informationen über verschlüsselte Geräte und den Verschlüsselungsstatus. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver.
- Details zu Fehlern bei Datenverschlüsselungen auf Geräten, die mit der Funktion zur Datenverschlüsselung von Kaspersky-Anwendungen ausgeführt wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.
- Liste der verwalteten speicherprogrammierbaren Steuerungen (SPS). Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Daten, die zur Erstellung einer Übersicht über die Ausbreitung einer Bedrohung benötigt werden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien der entsprechenden Anwendung.

- Informationen über Versuche von Unternehmensmitarbeitern, auf Cloud-Dienste zuzugreifen. Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Daten, die für die Integration von Kaspersky Security Center in Dienst von Kaspersky Managed Detection and Response erforderlich sind (das dedizierte Plug-In muss für Kaspersky Security Center Web Console installiert sein): Token der Initiierung der Integration, Token der Integration und Token der Benutzersitzung. Der Benutzer gibt den Token für die Initiierung der Integration in die Benutzeroberfläche der Kaspersky Security Center Web Console ein. Der Kaspersky MDR-Dienst überträgt die Token für die Integration und für die Benutzersitzung über das dedizierte Plug-In.

- Details der eingegebenen Aktivierungscodes oder angegebenen Schlüsseldateien. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- Benutzerkonten: Name, Beschreibung, vollständiger Name, E-Mail-Adresse, Haupttelefonnummer, Kennwort, vom Administrationsserver generierter geheimer Schlüssel und Einmalkennwort für die zweistufige Überprüfung. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- Daten, welche die Identitäts- und Zugriffsverwaltung für eine zentralisierte Authentifizierung und zur Bereitstellung von Single Sign-On (SSO) zwischen integrierten Kaspersky-Anwendungen und Kaspersky Security Center benötigt: Installations- und Konfigurationseinstellungen der Identitäts- und Zugriffsverwaltung, Benutzersitzung der Identitäts- und Zugriffsverwaltung, Token der Identitäts- und Zugriffsverwaltung, Statuswerte von Client-Programmen und Ressourcenservern. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- Revisionsverlauf von verwalteten Objekten. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- IP-Adresse des Geräts, auf dem eine Revision von einem Benutzer erstellt wurde. Die IP-Adresse wird vom Administrationsserver automatisch festgelegt.

- Register der gelöschten Managementobjekte. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- Aus der Datei erzeugte Installationspakete wie auch Installationseinstellungen. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center Web Console ein.

- Daten, die für die Anzeige für Neuigkeiten von Kaspersky in der Kaspersky Security Center Web Console erforderlich sind. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Daten, die für das Funktionieren von Plug-Ins verwalteter Anwendungen in Kaspersky Security Center Web Console erforderlich sind und die von den Plug-Ins in der Administrationsserver-Datenbank während ihres Regelbetriebs gespeichert werden. Die Beschreibung und Möglichkeiten zur Bereitstellung der Daten finden Sie in den Hilfedateien der entsprechenden Anwendung.

- Benutzereinstellungen für Kaspersky Security Center Web Console: Sprache und Schema der Benutzeroberfläche, Einstellungen für die Anzeige des Überwachungsfensters, Status der Benachrichtigungen (bereits gelesen / noch nicht gelesen), Status der Spalten in Tabellen (Eingeblendet / Ausgeblendet), Fortschritt des Trainingsmodus. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Das Kaspersky-Ereignisprotokoll für Komponenten von Kaspersky Security Center und von durch Kaspersky verwalteten Anwendungen. Das Kaspersky-Ereignisprotokoll wird auf jedem Gerät gespeichert und nie zum Administrationsserver übertragen.

- Zertifikat für eine sichere Verbindung zwischen verwalteten Geräten und Komponenten von Kaspersky Security Center. Mittels des Administrationsservers-Tools "klsetsrvcert" gibt der Benutzer Daten ein.

- Zertifikate zum Herstellen einer Vertrauensstellung für die internen Webressourcen des Unternehmens. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Daten, die für den Betrieb von Kaspersky Security Center in Cloud-Umgebungen wie Amazon Web Services (AWS), Microsoft Azure, Google Cloud und Yandex.Cloud erforderlich sind. Der Administrationsserver empfängt die Daten von der virtuellen Maschine, auf der er ausgeführt wird.

- Informationen über das Akzeptieren der Bedingungen von rechtlichen Vereinbarungen mit Kaspersky durch den Benutzer.

- Die Daten des Administrationsservers, die der Benutzer in die folgenden Komponenten eingibt:

  - Verwaltungskonsole

  - Kaspersky Security Center Web Console

  - Befehlszeilenterminal bei Verwendung des Tools "klscflag"

  - Komponenten, die mit dem Administrationsserver über "klakaut"-Automatisierungsobjekte und Kaspersky Security Center OpenAPI interagieren

- Alle vom Benutzer in die Benutzeroberfläche von der Verwaltungskonsole oder von Kaspersky Security Center Web Console eingegebenen Daten.

Die oben aufgeführten Daten können in Kaspersky Security Center vorhanden sein, wenn eine der folgenden Methoden angewendet wird:

- Der Benutzer gibt Daten in die Schnittstellen der folgenden Komponenten ein:

  - Verwaltungskonsole

  - Kaspersky Security Center Web Console

  - Befehlszeilenterminal bei Verwendung des Tools "klscflag"

  - Komponenten, die mit dem Administrationsserver über "klakaut"-Automatisierungsobjekte und Kaspersky Security Center OpenAPI interagieren

- Der Administrationsagent empfängt Daten automatisch vom Gerät und überträgt diese an den Administrationsserver.

- Der Administrationsagent empfängt von der durch Kaspersky verwalteten Anwendung abgerufenen Daten und überträgt sie an den Administrationsserver. Die Liste der verarbeiteten Daten von der durch Kaspersky verwalteten Anwendungen finden Sie in der Hilfe der entsprechenden Anwendungen.

- Der Administrationsserver ruft Informationen über die Geräte im Netzwerk selbstständig ab oder erhält Informationen von einem Administrationsagenten, der als Verteilungspunkt agiert.

- Daten werden vom mobilen Gerät zum Administrationsserver mittels iOS MDM-Protokoll übertragen.

Die aufgelisteten Daten werden in der Administrationsserver-Datenbank gespeichert. Benutzernamen und Kennwörter werden in verschlüsselter Form gespeichert.

Alle oben aufgeführten Daten, einschließlich Protokolldateien, die von Installationsprogrammen und Dienstprogrammen erstellt wurden, können nur mittels Dump-Dateien, Protokolldateien oder Log-Dateien von Komponenten von Kaspersky Security Center an Kaspersky übertragen werden.

Dump-Dateien, Protokolldateien und Log-Dateien von Komponenten des Kaspersky Security Centers enthalten zufällige Daten des Administrationsservers, des Administrationsagenten, der Verwaltungskonsole, des iOS MDM-Server und der Kaspersky Security Center Web Console. Diese Dateien können persönliche und vertrauliche Daten enthalten. Dump-Dateien, Protokolldateien und Log-Dateien werden unverschlüsselt auf dem Gerät gespeichert. Dump-Dateien, Protokolldateien und Log-Dateien werden nicht automatisch an Kaspersky übertragen. Der Administrator kann jedoch auf Anforderung des Technischen Supports Daten manuell an Kaspersky übertragen, um Probleme im Kaspersky Security Center zu beheben.

Durch folgen der Links in der Verwaltungskonsole oder der Kaspersky Security Center Web Console stimmt der Nutzer zu, die folgenden Daten automatisch zu übertragen:

- Code von Kaspersky Security Center
- Version von Kaspersky Security Center
- Lokalisierung der Kaspersky Security Center
- Lizenz-ID
- Lizenztyp
- Ob die Lizenz über einen Partner bezogen wurde

Die Liste an Daten, die über einen Link zur Verfügung gestellt werden, ist abhängig von Zweck und Standort des Links.

Kaspersky verwendet die erhaltenen Daten in anonymisierter Form und nur für allgemeine Statistiken. Zusammenfassende Statistiken werden automatisch aus den ursprünglich erhaltenen Informationen erstellt und enthalten keine persönlichen oder vertraulichen Daten. Sobald neue Daten akkumuliert wurden, werden die vorherigen Daten gelöscht (einmal pro Jahr). Zusammenfassende Statistiken werden unbegrenzt gespeichert.

Kaspersky schützt alle erhaltenen Informationen in Übereinstimmung mit den geltenden Gesetzen und geltenden Kaspersky-Regeln. Daten werden über einen sicheren Kanal übertragen.

Varianten der Lizenzierung von Kaspersky Security Center

Kaspersky Security Center besitzt folgende Ausführungsmodi:

- **Ohne Lizenz (Grundlegende Funktionen)**

  Kaspersky Security Center arbeitet in diesem Modus, bevor die Anwendung aktiviert wird oder nachdem die kommerzielle Lizenz abläuft. Die Anwendung Kaspersky Security Center, welche die Basisfunktionen der Verwaltungskonsole unterstützt, wird zusammen mit den Kaspersky-Produkten geliefert, die für den Schutz des Unternehmensnetzwerks konzipiert sind. Außerdem steht es auf der Website von Kaspersky zum Download bereit.

- **Kommerzielle Lizenz**

Wenn Sie zusätzliche Funktionen benötigen, die nicht zu den Grundfunktionen der Verwaltungskonsole gehören, müssen Sie eine kommerzielle Lizenz erwerben.

Stellen Sie beim Hinzufügen eines Lizenzschlüssels im Eigenschaftenfenster des Administrationsservers sicher, dass Sie den Lizenzschlüssel hinzufügen, mit dem sich Kaspersky Security Center verwenden lässt. Sie können diese Informationen auf der Kaspersky-Website finden. Die Websites der einzelnen Lösungen bieten eine Liste der Anwendungen, die in der jeweiligen Lösung enthalten sind. Der Administrationsserver akzeptiert möglicherweise nicht unterstützte Lizenzschlüssel, beispielsweise Lizenzschlüssel für Kaspersky Endpoint Security Cloud, aber diese Lizenzschlüssel bieten neben den grundlegenden Funktionen der Verwaltungskonsole keine neuen Funktionen.

Funktion oder Eigenschaft	Ausführungsmodus von Kaspersky Security Center	
	Keine Lizenz	Kommerzielle Lizenz
Basisfunktionen der Verwaltungskonsole Es stehen folgende Funktionen zur Verfügung: • Virtuelle Administrationsserver erstellen, um ein Netzwerk entfernter Standorte bzw. Kundenunternehmen zu verwalten • Hierarchie der Administrationsgruppen erstellen, um eine Reihe von Geräten als Ganzes zu verwalten • Remote-Installation von Anwendungen • Einstellungen der auf den Client-Geräten installierten Anwendungen zentral anpassen • Status der Antiviren-Sicherheit eines Unternehmens kontrollieren • Benutzerrollen verwalten • Statistiken und Berichte über die Ausführung von Anwendungen sowie Benachrichtigungen über kritische Ereignisse erhalten • Zentral Dateien verwalten, die in die Quarantäne, ins Backup oder in die Ablage für Dateien mit verschobener Verarbeitung verschoben wurden • Verschlüsselung und Datenschutz verwalten • Vorhandene lizenzierte Anwendungsgruppen anzeigen und ändern • Liste der durch eine Netzwerkabfrage gefundenen Geräte anzeigen und manuell bearbeiten • Liste der Betriebssystem-Abbilder anzeigen, die für die Remote-Installation verfügbar sind	✓	✓
Schwachstellen- und Patch-Management: Basisfunktionen Für die folgenden Aufgaben ist keine kommerzielle Lizenz erforderlich: • Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* Über die Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates erhält Kaspersky Security Center eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Drittanbieter-Programme, die auf den verwalteten Geräten installiert ist. • Aufgabe *Windows-Updates installieren* Diese Aufgabe kann nur zur Installation von Windows-Updates verwendet werden. Um diese Aufgabe zu verwenden, müssen Sie die erforderlichen Updates manuell in den Aufgabeneinstellungen angeben. • Aufgabe *Schwachstellen schließen* Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Software von Microsoft und individuelle Korrekturen für Drittanbieter-Programme. Um die Aufgabe zu verwenden, müssen Sie manuell individuelle Korrekturen angeben.	✓	✓
Schwachstellen- und Patch-Management: Erweiterte Funktionen Es stehen folgende Funktionen zur Verfügung: • Remote-Installation von Programm-Updates und automatisches Schließen von Schwachstellen gemäß den von Ihnen festgelegten Regeln. • Verwendung des Administrationsservers als WSUS-Server (Windows Server Update Services) zur Bereitstellung von Updates für die Windows Update-Dienste auf Geräten im zentralisierten Modus und mit festgelegter Häufigkeit.	—	✓

Funktion oder Eigenschaft	Ausführungsmodus von Kaspersky Security Center	
	Keine Lizenz	Kommerzielle Lizenz
Funktion zur Verwaltung mobiler Geräte in der MMC-basierten Verwaltungskonsole Die Funktion zur Verwaltung mobiler Geräte wird verwendet, um iOS MDM- und Android-Geräte zu verwalten. Für mobile iOS MDM-Geräte sind folgende Funktionen verfügbar: • Hinzufügen neuer Geräte unter die Verwaltung von Kaspersky Security Center. • Konfigurationsprofile erstellen und bearbeiten, Konfigurationsprofile auf mobilen Geräten installieren • Installation von Anwendungen auf mobilen Geräten durch den App Store®, durch die Verwendung von Manifest-Dateien (.plist) oder durch die Verwendung von mobilen Installationspaketen (.ipa). • Befehle auf iOS MDM-Geräten ausführen, einschließlich dem Sperren von mobilen Geräten, dem Zurücksetzen des Kennworts eines mobilen Geräts und dem Löschen aller Daten von einem mobilen Gerät. Für Android-Geräte sind folgende Funktionen verfügbar: • Hinzufügen neuer Geräte unter die Verwaltung von Kaspersky Security Center. • Verwaltung von Kaspersky Endpoint Security für Android über eine Richtlinie. • Befehle auf Geräten ausführen. Administrationseinheit für die Funktion zur Verwaltung mobiler Geräte ist das einzelne mobile Gerät. Ein mobiles Gerät gilt als verwaltet, sobald es zum Server für mobile Geräte verbunden wird.	—	✓ (Den Eigenschaften des Administrationsservers muss ein Lizenzschlüssel hinzugefügt werden.)
Schutz mobiler Geräte in der Kaspersky Security Center Web Console Kaspersky Security Center Web Console bietet Ihnen die folgenden Funktionen zur Verwaltung mobiler Android- und iOS-Geräte: • Hinzufügen neuer Geräte unter die Verwaltung von Kaspersky Security Center. • Verwaltung von Kaspersky Endpoint Security für Android und Kaspersky Security für iOS durch Richtlinien. • Senden von Befehlen an mobile Geräte mittels entsprechender Protokolle sowie das Ausführen von Befehlen.	—	✓ (Auf jedem mobilen Gerät muss ein Lizenzschlüssel hinzugefügt werden.)
Systemverwaltung Es stehen folgende Funktionen zur Verfügung: • Installation von Betriebssystemen und Programmen. Kaspersky Security Center ermöglicht das Erstellen und die Verteilung von Betriebssystem-Abbildern auf Client-Geräten eines Netzwerks sowie die Remote-Installation von Programmen von Kaspersky oder anderen Software-Herstellern. Sie können Betriebssystem-Images von Geräten erstellen und diese Images an den Administrationsserver übermitteln. Die dadurch erstellten Betriebssystem-Images werden in einem freigegebenen Ordner auf dem Administrationsserver gespeichert. Das Erstellen eines Betriebssystem-Images eines Mustergeräts erfolgt mit der Aufgabe zum Erstellen eines Installationspakets. Sie können die erstellten Images zur Bereitstellung auf neue Geräte des Netzwerks verwenden, auf denen noch kein Betriebssystem installiert wurde. Dazu wird die Technologie Preboot eXecution Environment (PXE) verwendet. • Lizenzierte Programmgruppen verwalten • Remote-Berechtigung für die Verbindung zu Client-Geräten durch eine Komponente von Microsoft® Windows® namens Remote Desktop Connection • Remote-Verbindung mit Client-Geräten über Windows Desktopfreigabe • Remote-Verbindung mittels **Kaspersky Remote Desktop Session Viewer**.	—	✓

Funktion oder Eigenschaft	Ausführungsmodus von Kaspersky Security Center	
	Keine Lizenz	Kommerzielle Lizenz
Integration mit Cloud-Umgebungen Kaspersky Security Center arbeitet nicht nur mit lokalen Geräten, sondern stellt auch spezielle Funktionen zum Arbeiten in einer Cloud-Umgebung, wie den Assistenten für das Konfigurieren der Cloud-Umgebung, bereit. Kaspersky Security Center arbeitet mit folgenden virtuellen Maschinen: • Amazon EC2-Instances • Virtuelle Maschinen in Microsoft Azure • Instanzen virtueller Maschinen in Google Cloud • Virtuelle Maschinen in Yandex.Cloud	—	✓
Exportieren von Ereignissen mittels Syslog-Protokoll in SIEM-Systeme. Gemäß dem Protokoll Syslog können beliebige Ereignisse, die auf dem Kaspersky Security Center Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, übertragen werden. Das Syslog-Protokoll ist ein Standardprotokoll für das Aufzeichnen von Nachrichten. Sie können es für den Export von Ereignissen ein beliebiges SIEM-System verwenden.	✓	✓

Besonderheiten der Lizenzverwaltung für Kaspersky Security Center und die verwalteten Programme

Bei der Lizenzverwaltung des Administrationsservers und der verwalteten Programme gelten folgende Besonderheiten:

- Zur Aktivierung der Funktionen von "Schwachstellen- und Patch-Management", "Verwaltung mobiler Geräte" oder "Integration mit SIEM-Systemen" können Sie auf einem Administrationsserver einen Lizenzschlüssel oder gültigen Aktivierungscode hinzufügen. Bestimmte Funktionen von Kaspersky Security Center sind nur in Abhängigkeit von aktiven Schlüsseldateien oder gültigen Aktivierungscodes verfügbar, die auf dem Administrationsserver hinzugefügt wurden.

- In der Datenverwaltung des Administrationsservers können Sie mehrere Aktivierungscodes und Schlüsseldateien für verwaltete Programme hinzufügen.

Besonderheiten der Lizenzverwaltung für Kaspersky Security Center

Wenn Sie z. B. die Funktionen von "Mobile Geräte verwalten" mithilfe einer Schlüsseldatei aktiviert haben, aber zusätzlich noch die Funktionen von "Schwachstellen- und Patch-Management" benötigen, müssen Sie bei Ihrem Dienstanbieter eine Schlüsseldatei kaufen, die beide Funktionalitäten aktiviert, und den Administrationsserver mit dieser Schlüsseldatei aktivieren.

Besonderheiten der Lizenzverwaltung für verwaltete Programme

Um die verwalteten Programme zu lizenzieren, können Sie automatisch oder auf andere Weise einen Aktivierungscode oder eine Schlüsseldatei verteilen. Folgende Methoden zur Verteilung eines Aktivierungscodes oder einer Schlüsseldatei sind möglich:

- Mittels automatischer Verteilung

Wenn Sie verschiedene verwaltete Anwendungen verwenden und eine bestimmte Schlüsseldatei oder Aktivierungscode an die Geräte verteilen möchten, verwenden Sie andere Methoden zur Verteilung des Aktivierungscodes oder der Schlüsseldatei.

Kaspersky Security Center erlaubt die automatische Verteilung der vorhandenen Lizenzschlüssel an die Geräte. Angenommen, in der Datenverwaltung des Administrationsservers befinden sich drei Lizenzschlüssel. Sie haben das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** für alle drei Lizenzschlüssel gewählt. Auf den Unternehmensgeräten ist eine Sicherheitsanwendung von Kaspersky installiert, z. B. Kaspersky Endpoint Security für Windows. Ein neues Gerät wurde entdeckt und erfordert die Bereitstellung eines Lizenzschlüssels. Das Programm ermittelt, dass für dieses Gerät z. B. zwei Lizenzschlüssel aus dem Speicher geeignet sind: Lizenzschlüssel *Key_1* und Lizenzschlüssel *Key_2*. Einer dieser Lizenzschlüssel wird an das Gerät verteilt. In diesem Fall kann nicht vorausgesagt werden, welcher der beiden Lizenzschlüssel an das Gerät bereitgestellt werden wird, da die automatische Verteilung von Lizenzschlüsseln keinerlei Aktivitäten des Administrators vorsieht.

Bei der Verteilung des Lizenzschlüssels an das Gerät erfolgt eine Zählung aller Geräte, für die dieser Schlüssel gilt. Sie müssen sicherstellen, dass die Anzahl der Geräte, an die der Lizenzschlüssel verteilt wird, die Lizenzbeschränkung nicht überschreitet. Falls die Anzahl der Geräte die Lizenzbeschränkung überschreitet, wird allen Geräten, die nicht durch die Lizenz abgedeckt sind, der Status *Kritisch* zugewiesen.

- Hinzufügen einer Schlüsseldatei oder eines Aktivierungscodes zum Installationspaket eines verwalteten Programms

  Wenn die Installation des verwalteten Programms mithilfe eines Installationspakets erfolgt, können Sie eine Schlüsseldatei oder einen Aktivierungscode im Installationspaket oder in der Richtlinie dieses Programms angeben. Der Lizenzschlüssel wird bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver an die verwalteten Geräte verteilt.

- Verteilung mithilfe der Aufgabe zum Hinzufügen eines Lizenzschlüssels für ein verwaltetes Programm

  Wenn Sie die Aufgabe zum Hinzufügen eines Lizenzschlüssels für verwaltete Programme verwenden, können Sie den Lizenzschlüssel auswählen, der an die Geräte verteilt werden soll, und die Geräte auf die von Ihnen bevorzugte Art auswählen, z. B. indem Sie eine Administrationsgruppe oder eine Geräteauswahl wählen.

- Manuelles Hinzufügen des Aktivierungscodes oder der Schlüsseldatei auf den Geräten.

Kaspersky-Anwendungen. Zentralisierte Bereitstellung

In diesem Abschnitt werden Methoden für die Remote-Installation bzw. Deinstallation von Kaspersky-Anwendungen auf Netzwerkgeräten beschrieben.

Bevor die Installation der Programme auf den Client-Geräten beginnt, müssen Sie sich vergewissern, dass die Hardware- und Softwarevoraussetzungen das Gerät den Anforderungen entsprechen.

Die Kommunikation des Administrationsservers mit den Client-Geräten wird durch den Administrationsagenten sichergestellt. Deshalb ist es erforderlich, den Administrationsagenten auf jedem Client-Gerät zu installieren, das mit dem System der zentralen Remote-Administration verbunden werden soll. Auf dem Gerät, auf dem der Administrationsserver installiert wurde, kann nur die Serverversion des Administrationsagenten verwendet werden. Sie gehört zum Administrationsserver und wird zusammen mit ihm installiert und deinstalliert. Der Administrationsagent muss auf diesem Gerät nicht installiert werden.

Der Administrationsagent wird genauso wie die Anwendungen installiert. Dabei kann die Installation im Remote-Betrieb oder lokal erfolgen. Bei einer zentralen Bereitstellung von Sicherheitsanwendungen über die Verwaltungskonsole können Sie den Administrationsagenten zusammen mit den Antiviren-Programmen installieren.

Die Administrationsagenten können sich je nach den Kaspersky-Anwendungen unterscheiden, mit denen sie interagieren. In einigen Fällen ist nur eine lokale Installation des Administrationsagenten möglich (für Details siehe die Handbücher der jeweiligen Anwendung). Sie müssen den Administrationsagenten nur einmal auf einem Client-Gerät installieren.

Die Verwaltung von Kaspersky-Anwendungen über die Verwaltungskonsole erfolgt mit Verwaltungs-Plug-ins. Um mittels Kaspersky Security Center den Zugriff auf die Programmverwaltung zu bekommen, muss deshalb das entsprechende Verwaltungs-Plug-in auf dem Arbeitsplatz des Administrators installiert werden.

Sie können eine Remote-Installation von Programmen aus dem Administrator-Arbeitsplatz im Hauptfenster von Kaspersky Security Center durchführen.

Um Programme im Remote-Betrieb zu installieren, erstellen Sie eine Aufgabe zur Remote-Installation.

Die angelegte Aufgabe zur Remote-Installation wird je nach dem eingestellten Zeitplan aufgerufen. Sie können den Installationsvorgang unterbrechen, indem Sie die Aufgabe manuell beenden.

Wenn bei der Remote-Installation einer Anwendung ein Fehler auftritt, stellen Sie sicher, dass die Anforderungen an die Gerätevorbereitung erfüllt sind.

Sie können den Fortschritt der Remote-Installation von Kaspersky-Anwendungen im Netzwerk mithilfe des Berichts über die Bereitstellung verfolgen.

Detaillierte Informationen zur Verwaltung der aufgeführten Anwendungen über Kaspersky Security Center finden Sie in den Handbüchern der entsprechenden Anwendungen.

Ersetzen von Sicherheitsanwendungen von Drittanbietern

Zur Installation der Sicherheitsanwendungen von Kaspersky mithilfe von Kaspersky Security Center ist es möglicherweise erforderlich, Drittanbieter-Programme zu löschen, die mit dem zu installierenden Programm nicht kompatibel ist. Kaspersky Security Center bietet mehrere Methoden zur Deinstallation von Drittanbieter-Programmen.

Inkompatible Programme mittels Installer entfernen

Diese Option ist nur in der Verwaltungskonsole auf Basis der Microsoft Management Console verfügbar.

Die Installationsmethode zum Entfernen inkompatibler Programme wird von verschiedenen Installationsarten unterstützt. Vor der Installation der Sicherheitsanwendungen werden die damit inkompatiblen Programme automatisch gelöscht, wenn im Eigenschaftenfenster des Installationspakets für die Sicherheitsanwendung (Abschnitt **Inkompatible Programme**) die Option **Inkompatible Programme automatisch entfernen** aktiviert ist.

Inkompatible Programme während der Konfiguration der Remote-Installation eines Programms entfernen

Sie können die Option **Inkompatible Programme automatisch entfernen** aktivieren, wenn Sie die Remote-Installation einer Sicherheitsanwendung konfigurieren. In der Verwaltungskonsole auf Basis der Microsoft Management Console (MMC) ist diese Option im Assistenten für Remote-Installationen verfügbar. In der Kaspersky Security Center Web Console finden Sie diese Option im Assistenten für die Bereitstellung des Schutzes. Wenn diese Option aktiviert ist, entfernt Kaspersky Security Center vor der Installation einer Sicherheitsanwendung auf dem verwalteten Gerät inkompatible Programme.

Anleitung:

- Verwaltungskonsole: Inkompatible Programme mit dem Assistenten für Remote-Installationen deinstallieren
- Kaspersky Security Center Web Console: Inkompatible Programme vor der Installation deinstallieren

Löschen der inkompatiblen Programme mithilfe einer separaten Aufgabe

Zum Löschen der inkompatiblen Anwendungen wird die Aufgabe **Remote-Deinstallation der Anwendung** verwendet. Die Aufgabe muss vor der Aufgabe zur Installation der Sicherheitsanwendung auf den Geräten gestartet werden. Beispielsweise kann in der Installationsaufgabe ein Zeitplan des Typs **Nach Beenden einer anderen Aufgabe** ausgewählt werden, wobei die andere Aufgabe die Aufgabe **Remote-Deinstallation der Anwendung** ist.

Die Verwendung dieser Löschmethode ist zweckmäßig, wenn der Installer der Sicherheitsanwendung eines der inkompatiblen Programme nicht erfolgreich löschen kann.

Anleitung für die Verwaltungskonsole: Erstellen einer Aufgabe.

Programme mit der Aufgabe zur Remote-Installation installieren

Kaspersky Security Center ermöglicht es, Programme auf den Geräten per Remote-Zugriff mithilfe der Aufgaben der Remote-Installation zu installieren. Mithilfe des Assistenten werden die Aufgaben erstellt und den Geräten zugewiesen. Um den Geräten schneller und einfacher eine Aufgabe zuzuweisen, können Sie die (bis zu 1.000) Geräte im Fenster des Assistenten auf die von Ihnen bevorzugte Art festlegen:

- **Geräte auswählen, die vom Administrationsserver erkannt wurden**. In diesem Fall wird die Aufgabe einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- **Geräteadressen manuell angeben oder aus Liste importieren**. Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.
- **Aufgabe einer Geräteauswahl zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine vordefinierte Auswahl oder Ihre eigene Auswahl angeben.
- **Aufgabe einer Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Administrationsgruppe gehören.

Um Probleme zu vermeiden, die während der Installation der Anwendung auf einem Client-Gerät ohne installierten Administrationsagent auftreten können, müssen Sie vorgehen, wie hier beschrieben: Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center.

Programm auf ausgewählten Geräten installieren

Um ein Programm auf ausgewählten Geräten zu installieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**, um die Erstellung der Aufgabe zu starten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** den Aufgabentyp **Remote-Installation des Programms** aus.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe zur Remote-Installation des gewählten Programms für die Reihe von Geräten erstellt. Die erstellte Aufgabe wird im Arbeitsbereich des Ordners **Aufgaben** angezeigt.

3. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm auf den gewählten Geräten installiert.

Programm auf den Client-Geräten einer Administrationsgruppe installieren

Um ein Programm auf Client-Geräten einer Administrationsgruppe zu installieren, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zu dem Administrationsserver her, der die gewünschte Administrationsgruppe verwaltet.

2. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus.

3. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Aufgaben** aus.

4. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**, um die Erstellung der Aufgabe zu starten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** den Aufgabentyp **Remote-Installation des Programms** aus.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Gruppenaufgabe zur Remote-Installation des gewählten Programms erstellt. Die erstellte Aufgabe wird im Arbeitsbereich der Administrationsgruppe auf der Registerkarte **Aufgaben** angezeigt.

5. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm auf den Client-Geräten der Administrationsgruppe installiert.

Programme mit Gruppenrichtlinien des Active Directory installieren

Mit Kaspersky Security Center können Sie Kaspersky-Anwendungen auf verwalteten Geräten mithilfe der Gruppenrichtlinien des Active Directory installieren. Das Gerät mit dem Administrationsserver muss sich in derselben Domäne wie die verwalteten Geräte befinden.

Sie können Programme mithilfe der Gruppenrichtlinien des Active Directory nur aus Installationspaketen installieren, die den Administrationsagenten enthalten.

Um ein Programm mithilfe von Gruppenrichtlinien des Active Directory zu installieren, gehen Sie wie folgt vor:

1. Beginnen Sie mit der Konfiguration der Programminstallation unter Verwendung des Assistenten für Remote-Installationen.
2. Aktivieren Sie im Fenster **Festlegen der Einstellungen der Aufgabe zur Remote-Installation** des Assistenten für Remote-Installationen die Option **Installation des Installationspakets in Active Directory-Gruppenrichtlinien festlegen**.
3. Wählen Sie die Option **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)** im Fenster **Benutzerkonten für den Zugriff auf Geräte auswählen** des Assistenten für Remote-Installationen.
4. Fügen Sie das entweder Benutzerkonto mit Administratorberechtigungen auf dem Gerät, auf dem Kaspersky Security Center installiert ist hinzu, oder das Benutzerkonto, das in der Domänengruppe der Group Policy Creators Owners beinhaltet ist.
5. Gewähren Sie dem ausgewählten Benutzerkonto die Berechtigungen:
   a. Gehen Sie zu **Systemsteuerung** → **Verwaltung** → **Verwaltung von Gruppenrichtlinien**.
   b. Klicken Sie auf den Knoten mit dem gewünschten Namen.
   c. Klicken Sie auf den Abschnitt **Delegieren**.
   d. Wählen Sie in der Dropdown-Liste **Berechtigung** die Option **GPOs verlinken** aus.
   e. Klicken Sie auf **Hinzufügen**.
   f. Wählen Sie im neuen Fenster **Benutzer, Computer oder Gruppe auswählen** das gewünschte Benutzerkonto.
   g. Klicken Sie auf **OK**, um das Fenster **Benutzer, Computer oder Gruppe auswählen** zu schließen.
   h. Wählen Sie in der Liste **Benutzer und Gruppen** das Konto, dass Sie gerade hinzugefügt haben und klicken Sie anschließend auf **Erweitert** → **Erweitert**.
   i. Doppelklicken Sie in der Liste **Berechtigungseinträge** auf das Konto, dass Sie gerade hinzugefügt haben.
   j. Gewähren Sie die folgenden Berechtigungen:
      - **Erstellen von Gruppenobjekten**
      - **Löschen von Gruppenobjekten**

- **Objekte für Gruppenrichtliniencontainer erstellen**
- **Objekte für Gruppenrichtliniencontainer löschen**

k. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

6. Legen Sie die weiteren Einstellungen fest, indem Sie den Anweisungen des Assistenten folgen.
7. Starten Sie die erstellte Aufgabe zur Remote-Installation manuell oder gemäß einem Zeitplan.

Daraufhin wird die Remote-Installation auf folgende Weise ausgeführt:

1. Nach dem Start der Aufgabe werden in jeder Domäne, zu der Client-Geräte für diese Aufgabe zur Remote-Installation gehören, folgende Objekte angelegt:
   - Group policy object (GPO) mit dem Namen **Kaspersky_AK{GUID}**.
   - Eine Sicherheitsgruppe, die dem GPO entspricht. Diese Sicherheitsgruppe umfasst Client-Geräte, auf die sich die Aufgabe erstreckt. Die Zusammensetzung der Sicherheitsgruppe bestimmt den Geltungsbereich des GPOs.
2. Kaspersky Security Center installiert die Kaspersky-Anwendungen auf den Client-Geräten direkt aus dem freigegeben Netzwerkordner "KLSHARE" der Anwendung. Im Installationsordner von Kaspersky Security Center wird dabei ein untergeordneter Hilfsordner erstellt, der die msi-Datei für das zu installierende Programm enthält.
3. Beim Hinzufügen neuer Geräte zum Gültigkeitsbereich der Aufgabe werden diese erst beim nächsten Start der Aufgabe zur entsprechenden Sicherheitsgruppe hinzugefügt. Wenn die Option **Übersprungene Aufgaben starten** aktiviert ist, werden die Geräte sofort zur Sicherheitsgruppe hinzugefügt.
4. Beim Löschen von Geräten aus dem Gültigkeitsbereich einer Aufgabe werden sie erst beim nächsten Start der Aufgabe aus der Sicherheitsgruppe gelöscht.
5. Beim Löschen einer Aufgabe aus dem Active Directory werden auch das GPO, der Link für das GPO und die entsprechende Sicherheitsgruppe gelöscht.

Wenn Sie ein anderes Installationsschema über Active Directory verwenden möchten, können Sie die Einstellungen manuell ändern. Das kann in folgenden Fällen nötig werden:

- Wenn der Administrator für den Antiviren-Schutz nicht die nötigen Rechte besitzt, um im Active Directory einiger Domänen Änderungen vorzunehmen.
- Wenn das ursprüngliche Installationspaket auf einer separaten Netzwerkressource gespeichert werden soll.
- Wenn ein GPO konkreten Unterabteilungen des Active Directory zugewiesen werden soll.

Folgende alternative Installationsschemata über Active Directory sind verfügbar:

- Falls die Installation direkt aus dem freigegebenen Ordner von Kaspersky Security Center erfolgen soll, muss in den Eigenschaften des GPO eine msi-Datei angegeben werden, die sich im exec-Unterordner des Ordners des Installationspakets für das erforderliche Programm befindet.
- Wenn das Installationspaket in einer anderen Netzwerkressource gespeichert werden muss, kopieren Sie den ganzen Inhalt des Ordners exec in das Paket, weil der Ordner neben der msi-Datei die Konfigurationsdateien enthält, die beim Anlegen des Installationspakets erstellt wurden. Um den Lizenzschlüssel zusammen mit dem Programm zu installieren, kopieren Sie auch die Schlüsseldatei in den Ordner.

Remote-Installation von Anwendungen auf macOS-Geräten

So installieren Sie Anwendungen auf Geräten mit macOS mithilfe einer Aufgabe zur Remote-Installation:

1. Erstellen Sie ein Archiv, das aus einem Installationspaket und einem .sh-Installationsskript besteht.
2. Deaktivieren Sie im Assistenten für das Erstellen einer Aufgabe die Option **Typ des Betriebssystems vor dem Download prüfen**.

Alternativ können Sie die Aufgabe **Skripte remote ausführen** verwenden. Im folgenden Artikel wird beschrieben, wie Sie Dateien für diese Aufgabe konfigurieren: Remote-Installation von Programmen auf Geräten mithilfe der Aufgabe zur Remote-Ausführung von Skripten.

Anwendungen auf sekundären Administrationsservern installieren

Um eine Anwendung auf sekundären Administrationsservern zu installieren:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten sekundären Administrationsserver verwaltet.
2. Vergewissern Sie sich, dass sich das zum Programm passende Installationspaket auf jedem der gewählten sekundären Administrationsserver befindet. Wenn es auf keinem der sekundären Server ein Installationspaket gibt, verteilen Sie es mithilfe der Aufgabe zur Verteilung des Installationspakets.
3. Starten Sie das Erstellen einer Aufgabe zur Installation eines Programms auf sekundären Administrationsservern auf eine der folgenden Arten:
   - Wenn Sie die Aufgabe für sekundäre Administrationsserver einer gewählten Administrationsgruppe erstellen möchten, starten Sie das Erstellen einer Gruppenaufgabe zur Remote-Installation für diese Gruppe.
   - Wenn Sie die Aufgabe für eine Auswahl von sekundären Servern erstellen möchten, starten Sie das Erstellen einer Aufgabe zur Remote-Installation für eine Reihe von Geräten.

   Daraufhin wird der Assistent für das Erstellen einer Aufgabe zur Remote-Installation gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** den Aufgabentyp **Remote-Installation des Programms auf den sekundären Administrationsservern** aus.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe zur Remote-Installation des gewählten Programms auf den gewählten sekundären Administrationsservern erstellt.
4. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm auf den gewählten sekundären Administrationsservern installiert.

Programme mit dem Assistenten für Remote-Installationen installieren

Bei der Installation von Kaspersky-Anwendungen können Sie den Assistenten für Remote-Installationen einsetzen. Der Assistent für Remote-Installationen ermöglicht die Remote-Installation der Programme mit zuvor angelegten Installationspaketen oder von den Programmpaketen.

Damit die Aufgabe Remote-Installation auf einem Client-Gerät, auf dem der Administrationsagent nicht installiert ist, korrekt ausgeführt wird, müssen die folgenden Ports geöffnet werden: TCP 139 und 445, sowie UDP 137 und 138. Diese Ports sind standardmäßig für alle Geräte offen, die zur Domäne gehören. Bei Netzwerkfehlern können Sie in der Wissensdatenbank von Kaspersky Security Center. nachschlagen.

Um ein Programm mithilfe des Assistenten für Remote-Installationen auf den ausgewählten Geräten zu installieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** den Unterordner **Installationspakete** aus.
2. Wählen Sie im Arbeitsbereich des Ordners das Installationspaket des Programms aus, das installiert werden soll.
3. Wählen Sie im Kontextmenü des Installationspakets die Option **Programm installieren** aus.

   Der Assistent für Remote-Installationen startet.
4. Im Fenster **Geräte für die Installation auswählen** kann eine Liste der Geräte erstellt werden, auf denen das Programm installiert werden soll:

   - **Auf Geräte in einer Gruppe von verwalteten Geräten installieren**

     Bei Auswahl dieser Option wird die Aufgabe zur Remote-Installation eines Programms für eine Gerätegruppe erstellt.

   - **Geräte für die Installation auswählen**

     Bei Auswahl dieser Option wird die Aufgabe zur Remote-Installation eines Programms für eine Reihe von Geräten erstellt. Dazu können verwaltete sowie nicht zugeordnete Geräte gehören.
5. Passen Sie im Fenster **Einstellungen für die Aufgabe zur Remote-Installation festlegen** die Einstellungen für die Remote-Installation eines Programms.

   Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Programminstallation erforderlichen Dateien auf die Client-Geräte aus:

   - **Unter Nutzung des Administrationsagenten**

     Wenn die Option aktiviert ist, werden die Installationspakete von dem auf den Client-Geräten installierten Administrationsagenten zugestellt.

     Wenn diese Option deaktiviert ist, werden Installationspakete mithilfe der Betriebssystems-Tools der Client-Geräte ausgeliefert.

     Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

     Diese Option ist standardmäßig aktiviert.

- **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**

  Wenn diese Option aktiviert ist, werden die Dateien durch den Administrationsserver mittels Betriebssystem-Tools der Client-Gerät auf die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

  Diese Option ist standardmäßig aktiviert.

- **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**

  Wenn diese Option aktiviert ist, werden Installationspakete mithilfe der Tools von den Betriebssystemen durch Verteilungspunkte auf die Geräte übertragen. Diese Variante ist wählbar, wenn sich im Netzwerk mindestens ein Verteilungspunkt befindet.

  Ist die Option **Mithilfe des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Betriebssystem-Tools zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

  Standardmäßig ist diese Option für die Aufgaben von Remote-Installationen aktiviert, die auf einem virtuellen Administrationsserver erstellt wurden.

  > Wenn alle Verteilungspunkte, die einem Gerät zugewiesen wurden, fehlerhaft sind, erhält das Gerät keine Updates (Antiviren-Datenbanken und Patches) und keine Installationspakete.

- **Anzahl der Installationsversuche**

  Wenn während einer Aufgabe zur Remote-Installation für Kaspersky Security Center die Anzahl an Installationsversuchen einer Anwendung auf einem verwalteten Gerät nicht innerhalb der Anzahl an Versuchen, die im Parameter angegeben wurde, erfolgreich ist, stoppt Kaspersky Security Center das Ausliefern des Installationspakets auf diesem verwalteten Gerät und startet die Installationsaufgabe auf dem Gerät nicht mehr.

  Mit der Option `Anzahl der Installationsversuche` können Sie die Ressourcen des verwalteten Geräts schonen und den Datenverkehr reduzieren (Deinstallation, MSI-Datei ausführen und Fehlermeldungen).

  Wiederholende Versuche zum Start der Aufgabe können auf ein Problem auf dem Gerät hinweisen, dass die Installation verweigert. Der Administrator sollte das Problem innerhalb der angegebenen Anzahl an Installationsversuchen lösen (z. B. durch das Zuweisen von ausreichend Speicherplatz, Entfernen von inkompatiblen Programmen oder Modifizieren von Einstellungen anderer Programme, welche die Installation verhindern) und die Aufgabe neu starten (manuell oder nach Zeitplan).

  Wenn die Installation nicht abgeschlossen werden kann, ist das Problem unter Umständen nicht lösbar und jeder weitere Aufgabenstart wird als kostspielig im Sinne unnützen Verbrauchs von Ressourcen und Datenverkehr betrachtet.

  Beim Erstellen der Aufgabe wird der Zähler auf `0` gesetzt. Jede Ausführung des Installers, die einen Fehler zurückliefert erhöht den Zählerstand.

  Wenn die im Parameter angegebene Anzahl an Versuchen überschritten wurde und das Gerät für die Installation der Anwendung bereit ist, können Sie den Wert der `Anzahl der Installationsversuche` erhöhen und die Aufgabe zu Installation der Anwendung starten. Alternativ können Sie eine neue Aufgabe zur Remote-Installation erstellen.

Legen Sie fest, wie Sie mit den durch den Administrationsserver verwalteten Client-Geräten verfahren möchten:

- **Auf allen Geräten installieren**

  Wird die Anwendung selbst auf den Geräten installiert, die von anderen Administrationsservern verwaltet werden.

  Diese Variante ist standardmäßig festgelegt. Sie müssen diese Einstellung nicht ändern, wenn Sie nur einen Administrationsserver in Ihrem Netzwerk haben.

- **Nur auf Geräten installieren, die durch diesen Administrationsserver verwaltet werden**

  Wird die Anwendung nur auf den Geräten installiert, die von diesem Administrationsserver verwaltet werden. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk mehrere Administrationsserver haben und Konflikte zwischen diesen vermeiden möchten.

Passen Sie die erweiterten Einstellungen an:

- **Anwendung nicht neu installieren, wenn sie bereits installiert ist**

  Wenn diese Option aktiviert ist, wird die ausgewählte Anwendung nicht neu installiert, wenn es bereits auf dem Client-Gerät installiert ist.

  Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Anwendung in jedem Fall installiert.

  Diese Option ist standardmäßig aktiviert.

- **Installation des Installationspakets in Active Directory-Gruppenrichtlinien festlegen**

  Wenn diese Option aktiviert ist, wird das Installationspaket mithilfe von Richtlinien des Active Directory installiert.

  Die Option ist verfügbar, wenn ein Installationspaket des Administrationsagenten ausgewählt ist.

  Diese Option ist standardmäßig deaktiviert.

6. Wählen Sie im Fenster **Lizenzschlüssel auswählen** einen Lizenzschlüssel und eine Verteilungsmethode aus:

- **Lizenzschlüssel nicht in das Installationspaket integrieren (empfohlen)**

  Der Schlüssel wird automatisch auf alle Geräte verteilt, mit denen er kompatibel ist:
  - Wenn in den Eigenschaften des Schlüssel die automatische Verteilung aktiviert ist.
  - Wenn die Aufgabe **Schlüssel hinzufügen** erstellt wurde.

- **Lizenzschlüssel im Installationspaket integrieren**

  Der Schlüssel wird gemeinsam mit dem Installationspaket an Geräte verteilt.

  > Es wird nicht empfohlen, den Schlüssel auf diese Art zu verteilen, da die Datenverwaltung der Installationspakete über allgemeinen Lesezugriff verfügt.

Das Fenster **Lizenzschlüssel auswählen** wird angezeigt, wenn das Installationspaket keinen Lizenzschlüssel enthält.

Wenn der Lizenzschlüssel zum Installationspaket gehört, wird das Fenster **Lizenzschlüssel-Einstellungen** mit Informationen über den Lizenzschlüssel angezeigt.

7. Legen Sie im Fenster **Methode zum Neustart des Betriebssystems** fest, ob das Gerät neu gestartet werden soll, wenn während der Programminstallation darauf ein Neustart des Betriebssystems erforderlich ist:

   - **Gerät nicht neu starten**

     Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung nicht neu gestartet.

   - **Gerät neu starten**

     Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung neu gestartet.

   - **Benutzer fragen**

     Bei dieser Option wird nach der Installation der Sicherheitsanwendung eine Meldung angezeigt, die den Benutzer auffordert, einen Neustart des Geräts durchzuführen. Durch Klicken auf den Link **Ändern** können Sie den Meldungstext ändern sowie das Intervall, in dem die Meldung angezeigt wird, und die Zeitdauer des automatischen Neustarts anpassen.

     Diese Variante ist standardmäßig ausgewählt.

   - **Beenden von Programmen in blockierten Sitzungen erzwingen**

     Wenn diese Option aktiviert ist, werden Anwendungen auf einem gesperrten Gerät vor dem Neustart zum Beenden gezwungen.

     Diese Option ist standardmäßig deaktiviert.

8. Im Fenster **Benutzerkonten für den Zugriff auf Geräte auswählen** können Benutzerkonten hinzugefügt werden, die für den Start der Aufgabe zur Remote-Installation verwendet werden sollen:

   - **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

     Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm der Anwendung gestartet werden soll. Die Aufgabe wird unter dem Konto gestartet, unter dem der Dienst des Administrationsservers läuft.

     Wenn der Administrationsagent nicht auf den Client-Geräten installiert ist, steht diese Option nicht zur Verfügung.

   - **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**

     Wählen Sie diese Option, wenn auf den Geräten, denen Sie die Aufgabe zur Remote-Installation zuweisen, der Administrationsagent nicht installiert ist. In diesem Fall können Sie ein Benutzerkonto oder ein SSH-Zertifikat angeben, um die Anwendung zu installieren.

     - **Lokales Benutzerkonto**. Wenn Sie diese Variante auswählen, können Sie das Benutzerkonto angeben, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Benutzerkonto** aus, und geben Sie anschließend die Anmeldeinformationen des Benutzerkontos an.

       Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Benutzerkonto existiert, dass über die erforderlichen Rechte auf allen Geräten verfügt, für welche die Aufgabe bestimmt wurde. In diesem Fall werden für den Start der Aufgabe alle hinzugefügten Konten nacheinander von oben nach unten angewandt.

     - **SSH-Zertifikat**. Wenn Sie eine Anwendung auf einem Linux-basierten Client-Gerät installieren möchten, können Sie anstelle eines Benutzerkontos ein SSH-Zertifikat angeben. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **SSH-Zertifikat** aus, und geben Sie anschließend den privaten und den öffentlichen Schlüssel des Zertifikats an.

Um einen privaten Schlüssel zu generieren, können Sie das Tool "ssh-keygen" verwenden. Beachten Sie, dass die Kaspersky Security Center das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" den Parameter "-m PEM" hinzu. Beispielsweise:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "< Benutzer-E-Mail >"
```

9. Klicken Sie im Fenster **Installation starten** auf die Schaltfläche **Weiter**, um die Aufgabe zur Remote-Installation auf den gewählten Geräten zu erstellen und zu starten.

   Ist im Fenster **Installation starten** die Option **Aufgabe nach Abschließen des Assistenten für Remote-Installationen nicht starten** aktiviert, so wird die Aufgabe zur Remote-Installation nicht gestartet. Später können Sie diese Aufgabe manuell starten. Der Aufgabenname entspricht dem Namen des Installationspakets für die Installation des Programms: **Installation <Name des Installationspakets>**.

Um ein Programm auf Geräten in der Administrationsgruppe mithilfe des Assistenten für Remote-Installationen zu installieren, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zu dem Administrationsserver her, der die gewünschte Administrationsgruppe verwaltet.

2. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus.

3. Klicken Sie im Arbeitsbereich der Gruppe auf die Schaltfläche **Aktion ausführen** und wählen Sie in der Dropdown-Liste die Option **Programm installieren**.

   Daraufhin wird der Assistent für Remote-Installationen gestartet. Folgen Sie den Anweisungen des Assistenten.

4. Klicken Sie im letzten Schritt des Assistenten auf die Schaltfläche **Weiter**, um die Aufgabe zur Remote-Installation auf den gewählten Geräten zu erstellen und zu starten.

Als Ergebnis der Ausführung des Assistenten für Remote-Installationen führt Kaspersky Security Center folgende Aktionen aus:

- Erstellt ein Installationspaket für das Programm (wenn es zuvor nicht erstellt wurde). Das Installationspaket wird im Ordner **Remote-Installation** im Unterordner **Installationspakete** mit dem Namen gespeichert, der dem Namen und der Version des Programms entspricht. Dieses Installationspaket kann zur weiteren Installation des Programms herangezogen werden.

- Erstellen und starten eine Aufgabe zur Remote-Installation für eine Reihe von Geräten oder für eine Administrationsgruppe. Die erstellte Aufgabe zur Remote-Installation wird im Ordner **Aufgaben** abgelegt und zu den Aufgaben der Administrationsgruppe hinzugefügt, für die sie erstellt wurde. Später können Sie diese Aufgabe manuell starten. Der Aufgabenname entspricht dem Namen des Installationspakets für die Installation des Programms: **Installation <Name des Installationspakets>**.

Umgang mit Verwaltungs-Plug-ins

Die Verwaltung von Kaspersky-Anwendungen über die Verwaltungskonsole erfolgt mithilfe von Verwaltungs-Plug-ins. Alle Kaspersky-Anwendungen, die über Kaspersky Security Center verwaltet werden können, umfassen ein Verwaltungs-Plug-in. Mithilfe des Plug-ins für die Programmverwaltung können Sie über die Verwaltungskonsole folgende Aktionen ausführen:

- Richtlinien, Einstellungen und Aufgabeneinstellungen von Programmen erstellen und bearbeiten.
- Informationen über Programmaufgaben und Ereignisse, die während der Programmausführung auftreten, sowie Statistiken zur Programmausführung von Client-Geräten abrufen.

So prüfen Sie die Liste der installierten Plug-ins und deren Versionen:

1. Klicken Sie in der Struktur der Verwaltungskonsole mit der rechten Maustaste auf **Administrationsserver <Name des Servers>** und wählen Sie **Eigenschaften** aus.
2. Klicken Sie auf **Erweitert** → **Informationen über installierte Programmverwaltungs-Plug-Ins**.

Im rechten Bereich wird die Liste der installierten Verwaltungs-Plug-ins mit ihren Versionen angezeigt.

Sie können die Plug-ins für verwaltete Programme installieren, indem Sie während der Erstkonfiguration von Kaspersky Security Center den Schnellstartassistenten des Administrationsservers ausführen. Sie können die Verwaltungs-Plug-ins ebenso manuell installieren.

So installieren Sie ein Verwaltungs-Plug-in manuell:

1. Laden Sie das Verwaltungs-Plug-in für die Kaspersky-Anwendung in der erforderlichen Version (z. B. Kaspersky Endpoint Security für Windows 12.6) von der Webseite des Technischen Supports von Kaspersky herunter.
2. Wenn die Verwaltungskonsole ausgeführt wird, schließen Sie diese.
3. Entpacken Sie die heruntergeladene Plug-in-Datei und starten Sie die Datei "klcfginst.msi" oder "klcfginst.exe". Folgen Sie den Anweisungen des Installationsassistenten.
4. Starten Sie nach Abschluss der Installation die Verwaltungskonsole und vergewissern Sie sich, wie im vorherigen Verfahren beschrieben, dass das Plug-in in der Liste der installierten Plug-ins aufgeführt ist.

Wenn Sie die Verwaltungskonsole nach der Installation eines Verwaltungs-Plug-ins ausführen, das den Schnellstartassistenten für verwaltete Programme unterstützt, wird dieser Assistent automatisch gestartet. Sie können die Schritte des Schnellstartassistenten für verwaltete Programme durchlaufen, um standardmäßige Richtlinien und Aufgaben für Kaspersky-Anwendungen zu erstellen. Der Assistent wird nur automatisch gestartet, wenn Sie die Verwaltungskonsole nach der Erstinstallation des Plug-ins starten oder das Verwaltungs-Plug-in auf eine Version aktualisieren, die mit einer anderen Version der Kaspersky-Anwendung kompatibel ist, für die noch keine Aufgaben und Richtlinien erstellt wurden. Sie können den Schnellstartassistenten für verwaltete Programme auch manuell starten.

So starten Sie den Schnellstartassistenten für verwaltete Programme manuell:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten des Administrationsservers und wählen Sie **Alle Aufgaben → Schnellstartassistent für das verwaltete Programm**.
3. Der Schnellstartassistent für verwaltete Programme wird gestartet. Folgen Sie den Schritten des Assistenten, um standardmäßige Richtlinien und Aufgaben für Kaspersky-Anwendungen zu erstellen.

So entfernen Sie ein Verwaltungs-Plug-in:

1. Wenn die Verwaltungskonsole ausgeführt wird, schließen Sie diese.
2. Öffnen Sie den Registry-Editor von Windows.
3. Suchen Sie den folgenden Schlüssel:
   - Für 32-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins`.
   - Für 64-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins`.

   Der Schlüssel enthält installierte Verwaltungs-Plug-ins. Für jedes Plug-in enthält der Wert `DisplayName` den Namen des Plug-ins und der Wert `UninstallString` den Befehl zum Deinstallieren des Plug-ins.
4. Suchen Sie den Schlüssel für das Plug-in, das Sie deinstallieren möchten, und kopieren Sie den Wert aus dessen `UninstallString` in die Zwischenablage.
5. Fügen Sie den Wert in die Befehlszeile ein und führen Sie ihn mit den Rechten des Systemadministrators aus.

Die Version des Verwaltungs-Plug-ins darf nicht älter als die Version des von Kaspersky verwalteten Programms sein. Wenn Sie die Kaspersky-Anwendung auf den Geräten aktualisieren, müssen Sie ebenfalls das Verwaltungs-Plug mit derselben Version installieren.

Wenn Sie eine Richtlinie öffnen, die in einer früheren Version des Plug-ins erstellt wurde, werden Sie aufgefordert, die Erklärung zu Kaspersky Security Network zu akzeptieren.

Bei einer Deinstallation der Kaspersky Security Center Web Console werden auch alle Verwaltungs-Plug-ins deinstalliert.

Wenn Sie eine Richtlinie in einer Plug-in-Version öffnen, die höher ist als die Version des verwalteten Programms, und anschließend speichern, wird die Richtlinie aktualisiert. Die Richtlinie kann anschließend nicht mehr in einem Plug-in einer früheren Version geöffnet werden.

Bericht über die Bereitstellung des Schutzes anzeigen

Um den Fortschritt der Bereitstellung des Schutzes im Netzwerk zu verfolgen, nutzen Sie den Bericht über die Bereitstellung des Schutzes.

Um den Bericht über die Bereitstellung des Schutzes anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie im Arbeitsbereich der Registerkarte **Berichte** die Berichtsvorlage **Bericht über die Bereitstellung des Schutzes** aus.

Im Arbeitsbereich wird daraufhin ein Bericht erstellt, der Daten über die Bereitstellung des Schutzes auf allen Geräten des Netzwerks enthält.

Sie können einen neuen Bericht über die Verteilung erstellen und angeben, welche Art von Daten darin enthalten sein soll:

- für eine Administrationsgruppe
- für eine Reihe von Geräten
- für die Geräteauswahl
- für alle Geräte

Im Rahmen von Kaspersky Security Center wird davon ausgegangen, dass der Schutz auf dem Gerät dann aktiv ist, wenn eine Sicherheitsanwendung installiert und der Echtzeitschutz eingeschaltet ist.

Remote-Deinstallation von Programmen

Kaspersky Security Center ermöglicht es, Programme von den Geräten per Remote-Zugriff mithilfe der Aufgaben der Remote-Deinstallation zu deinstallieren. Mithilfe des Assistenten werden die Aufgaben erstellt und den Geräten zugewiesen. Um den Geräten schneller und einfacher eine Aufgabe zuzuweisen, können Sie die Geräte im Fenster des Assistenten auf die von Ihnen bevorzugte Art festlegen:

- **Geräte auswählen, die vom Administrationsserver erkannt wurden**. In diesem Fall wird die Aufgabe einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- **Geräteadressen manuell angeben oder aus Liste importieren**. Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

- **Aufgabe einer Geräteauswahl zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine vordefinierte Auswahl oder Ihre eigene Auswahl angeben.

- **Aufgabe einer Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Administrationsgruppe gehören.

Probleme bei Remote-Deinstallationen

Wenn Sie die Remote-Deinstallation einer Drittanbieter-Anwendung ausführen, wird dem Administrator möglicherweise die folgende Warnung angezeigt: "Die Remote-Deinstallation wurde auf diesem Gerät mit Warnungen abgeschlossen: Die zu entfernende Anwendung ist nicht installiert." Dieses Problem tritt normalerweise auf, wenn die zu entfernende Anwendung nur für einen einzelnen Benutzer installiert ist, der aktuell angemeldet ist. Wenn der Benutzer nicht angemeldet ist, wird eine solche Anwendung unsichtbar und kann nicht gezielt per Fernzugriff deinstalliert werden.

Dieses Verhalten unterscheidet sich von Anwendungen, die von mehreren Benutzern auf demselben Gerät verwendet werden, wobei die Anwendungen für alle Benutzer des Geräts global sichtbar und zugänglich sind.

Der in Kaspersky Security Center enthaltene Algorithmus für die Programm-Registry behandelt Anwendungen für einzelne Benutzer und Anwendungen für mehrere Benutzer unterschiedlich:

- Anwendungen für mehrere Benutzer werden in einer stets aktuellen Liste der installierten Anwendungen in Echtzeit verwaltet.

- Die Anwendungen einzelner Benutzer werden mithilfe eines Caching-Mechanismus überwacht.

  Wenn ein Benutzer zum Zeitpunkt der Erkennung der Anwendung angemeldet war, speichert Kaspersky Security Center die Informationen über die Anwendungen des Benutzers im Cache. Auch wenn sich der Benutzer anschließend abmeldet, zeigt Kaspersky Security Center diese Anwendungen auf Grundlage der Daten im Cache weiterhin als installiert an, obwohl sie auf dem Gerät nicht mehr sichtbar oder zugänglich sind.

Diese Diskrepanz kann dazu führen, dass Kaspersky Security Center eine Anwendung aufgrund der gecachten Daten als installiert erkennt, die Deinstallation jedoch fehlschlägt, da die Anwendung bei abgemeldetem Benutzer nicht zugänglich ist.

Die Lebensdauer gecachter Daten beträgt standardmäßig 30 Tage. Administratoren können diese Einstellung ändern und die Cache-Dauer reduzieren. Auf diese Weise werden die Diskrepanzen zwischen den angezeigten Daten und der tatsächlichen Sichtbarkeit der Anwendung auf den Geräten minimiert.

Um die Lebensdauer des Cache auf 1 Stunde (3600 Sekunden) einzustellen, führen Sie auf dem Administrationsserver den folgenden Befehl aus:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

Damit die Änderungen wirksam werden, müssen Sie den Administrationsserver nach dem Ausführen dieses Befehls neu starten.

Informationsquellen zu installierten Anwendungen

Auf Windows-Geräten ruft der Administrationsagent Informationen über installierte Software aus den folgenden Registrierungsschlüsseln ab:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für alle Benutzer installiert sind.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für alle Benutzer installiert sind.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für den aktuellen Benutzer installiert sind.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für bestimmte Benutzer installiert sind.

Remote-Deinstallation eines Programms von den Client-Geräten einer Administrationsgruppe

Um ein Programm von den Client-Geräten einer Administrationsgruppe im Remote-Betrieb zu deinstallieren, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zu dem Administrationsserver her, der die gewünschte Administrationsgruppe verwaltet.

2. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus.

3. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Aufgaben** aus.

4. Klicken Sie auf die Schaltfläche **Neue Aufgabe**, um die Erstellung der Aufgabe zu starten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** den Aufgabentyp **Remote-Deinstallation des Programms** aus.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Gruppenaufgabe zur Remote-Deinstallation des gewählten Programms erstellt. Die erstellte Aufgabe wird im Arbeitsbereich der Administrationsgruppe auf der Registerkarte **Aufgaben** angezeigt.

5. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Deinstallation wird das gewählte Programm von den Client-Geräten der Administrationsgruppe entfernt.

Remote-Deinstallation eines Programms von den gewählten Geräten

Um ein Programm von den ausgewählten Geräten per Remote-Zugriff zu deinstallieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Starten Sie das Erstellen der Aufgabe durch Klick auf **Neue Aufgabe**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** den Aufgabentyp **Remote-Deinstallation des Programms** aus.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe zur Remote-Deinstallation des gewählten Programms für die Reihe von Geräten erstellt. Die erstellte Aufgabe wird im Arbeitsbereich des Ordners **Aufgaben** angezeigt.
3. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm von den ausgewählten Geräten entfernt.

Verwendung von Installationspaketen

Beim Erstellen von Aufgaben zur Remote-Installation werden Installationspakete eingesetzt, welche die Einstellungen enthalten, die für die Installation eines Programms benötigt werden.

> Installationspakete können die Schlüsseldatei beinhalten. Es ist nicht empfehlenswert, die Installationspakete mit der Schlüsseldatei mit allgemeiner Leseberechtigung zu verteilen.

Sie können dasselbe Installationspaket mehrmals verwenden.

Die vom Administrationsserver erstellten Installationspakete befinden sich in der Konsolenstruktur im Ordner **Remote-Installation** im Unterordner **Installationspakete**. Auf dem Administrationsserver werden die Installationspakete im angegebenen gemeinsamen Ordner im Unterordner "Packages" gespeichert.

Bei Bedarf können Sie ein Installationspaket aus dem Unterordner **Installationspakete** löschen, indem Sie den Anweisungen dieses Artikels folgen: Löschen eines Objekts.

> Ändern Sie den Inhalt von Installationspaketen in einem freigegebenen Ordner nicht selbstständig. Bei Bedarf können Sie von einem Installationspaket eine Kopie anlegen, in dieser die erforderlichen Änderungen vornehmen und anschließend neue Aufgaben zur Installation erstellen.

Installationspaket erstellen

Dieser Artikel beschreibt das Verfahren zur Erstellung von Installationspaketen der folgenden Arten:

- Installationspaket für eine Kaspersky-Anwendung
- Installationspaket für eine angegebene ausführbare Datei
- Installationspaket für eine Anwendung aus der Kaspersky-Datenbank

Für die Remote-Installation des Administrationsagenten müssen Sie kein Installationspaket manuell erstellen. Es wird während der Installation von Kaspersky Security Center automatisch erstellt und im Ordner **Installationspakete** gespeichert. Wenn das Paket für die Remote-Installation des Administrationsagenten gelöscht wurde, können Sie es erneut erstellen, indem Sie im Ordner "NetAgent" des Programmpakets von Kaspersky Security Center die Datei "nagent.kud" auswählen.

So erstellen Sie ein Installationspaket:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur die Option **Erweitert → Remote-Installation → Installationspakete**.
3. Starten Sie den Vorgang zum Erstellen eines neuen Installationspakets auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf den Ordner **Installationspakete** und wählen Sie anschließend im Kontextmenü die Option **Neu → Installationspaket**.
   - Klicken Sie mit der rechten Maustaste in den leeren Bereich der Liste mit den Installationspaketen und wählen Sie anschließend im Kontextmenü die Option **Erstellen → Installationspaket**.
   - Klicken Sie im Verwaltungsbereich der Liste mit den Installationspaketen auf die Option **Installationspaket erstellen**.

   Der Assistent für neue Installationspakete wird gestartet.
4. Wählen Sie einen der folgenden Typen an Installationspaketen aus, indem Sie auf das entsprechende Symbol klicken:
   - Installationspaket für eine Kaspersky-Anwendung.
   - Installationspaket für eine angegebene ausführbare Datei.
   - Installationspaket für eine Anwendung aus der Kaspersky-Datenbank.
5. Geben Sie den Namen des zu erstellenden Installationspakets ein.

   Sie können einen beliebigen Namen angeben.

6. Wählen Sie die Anwendung oder ausführbare Datei, für die das Installationspaket erstellt werden soll, auf eine der folgenden Arten aus:

   - Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie im Windows-Standardfenster **Öffnen** ein auf den Datenträgern verfügbares Programmpaket der benötigten Anwendung aus.

     Diese Option kann verwendet werden, wenn Sie ein Installationspaket für eine Kaspersky-Anwendung oder für eine bestimmte ausführbare Datei erstellen möchten.

   - Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie im Fenster **Anwendung auswählen** das Programmpaket der benötigten Anwendung aus.

     Diese Option kann verwendet werden, wenn Sie ein Installationspaket für eine Anwendung aus der Kaspersky-Datenbank erstellen möchten.

   Wenn Sie ein Installationspaket für den Administrationsserver erstellen möchten, wählen Sie die Datei "sc.kud" aus. Die Datei "sc.kud" befindet sich im Stammordner des Programmpakets für Kaspersky Security Center.

   Geben Sie in den Einstellungen der Installationspakete keine Daten von privilegierten Benutzerkonten an.

7. Machen Sie sich mit dem Endbenutzer-Lizenzvertrag und der Datenschutzrichtlinie vertraut.

   Wenn Sie ein Installationspaket für eine Anwendung erstellen, werden Sie möglicherweise aufgefordert, den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie für diese Anwendung anzuzeigen und zu akzeptieren.

   Lesen Sie sich beide Dokumente durch. Wenn Sie mit allen Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, akzeptieren Sie diese durch das Aktivieren der entsprechenden Kontrollkästchen.

   Die Installation der Anwendung auf Ihrem Gerät und die Erstellung des Installationspakets werden fortgesetzt.

   Wenn Sie ein Installationspakets für Kaspersky Endpoint Security for Mac erstellen, können Sie für den Lizenzvertrag und die Datenschutzrichtlinie die Sprache wählen.

8. Aktivieren Sie bei Bedarf die automatische Installation von Systemkomponenten.

   Wenn Sie für eine Anwendung aus der Kaspersky-Datenbank ein Installationspaket erstellen, können Sie die automatische Installation der erforderlichen Systemkomponenten aktivieren. Der Assistent für das Erstellen eines Installationspakets zeigt die Liste aller Systemkomponenten für die gewählte Anwendung an. Auf die Liste kann später jederzeit in den Eigenschaften des Installationspakets zugegriffen werden.

   Wenn Sie ein Installationspaket für einen Patch erstellen, enthält die Liste alle Systemkomponenten, die für die Bereitstellung dieses Patches erforderlich sind.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Erstellungsvorgang des Pakets abzuschließen

Sobald der Assistenten für das Erstellen eines Installationspakets abgeschlossen wurde, wird das erstellte Installationspaket in der Konsolenstruktur im Arbeitsbereich des Ordners **Installationspakete** angezeigt.

Autonome Installationspakete erstellen

Sie und die Gerätebenutzer in Ihrem Unternehmen können autonome Installationspakete verwenden, um Anwendungen manuell auf Geräten zu installieren.

Ein autonomes Installationspaket ist eine ausführbare Datei (installer.exe). Sie können diese Datei auf dem Webserver oder in einem freigegebenen Ordner speichern, oder auf andere Weise an ein Client-Gerät übertragen. Außerdem können Sie per E-Mail einen Link für das autonome Installationspaket senden. Auf dem Client-Gerät kann der Benutzer die empfangene Datei lokal ausführen, um ohne Beteiligung von Kaspersky Security Center eine Anwendung zu installieren.

Stellen Sie sicher, dass unbefugte Personen keinen Zugriff auf das autonome Installationspaket haben.

Sie können jetzt autonome Installationspakete für Kaspersky-Anwendungen und von Drittanbietern für Windows-, macOS- und Linux-Plattformen erstellen. Um ein autonomes Installationspaket für ein Drittanbieter-Programm zu erstellen, müssen Sie zuerst ein benutzerdefiniertes Installationspaket erstellen.

Als Quelle zum Erstellen von autonomen Installationspaketen dient die Liste der erstellten Installationspakete auf dem Administrationsserver.

So erstellen Sie ein autonomes Installationspaket:

1. Wählen Sie in der Konsolenstruktur **Administrationsserver → Erweitert → Remote-Installation → Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Wählen Sie in der Liste der Installationspakete das Installationspaket aus, für das Sie ein autonomes Paket erstellen möchten.

3. Wählen Sie im Kontextmenü den Punkt **Autonomes Installationspaket erstellen** aus.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

4. Wenn Sie auf der ersten Seite des Assistenten ein Installationspaket für die Kaspersky-Anwendung ausgewählt haben und den Administrationsagenten zusammen mit der ausgewählten Anwendung installieren möchten, stellen Sie sicher, dass die Option **Administrationsagent gemeinsam mit diesem Programm installieren** ist aktiviert.

   Diese Option ist standardmäßig aktiviert. Wir empfehlen, diese Option zu aktivieren, wenn Sie nicht sicher sind, ob der Administrationsagent auf dem Gerät installiert ist. Falls der Administrationsagent bereits auf dem Gerät installiert ist, wird der Administrationsagent auf die neue Version aktualisiert, nachdem das autonome Installationspaket mit dem Administrationsagenten installiert wurde.

   Wenn Sie diese Option deaktivieren, wird der Administrationsagent nicht auf dem Gerät installiert und das Gerät wird nicht verwaltet.

   Falls auf dem Administrationsserver bereits ein autonomes Installationspaket für die ausgewählte Anwendung vorhanden ist, werden Sie vom Assistenten darüber informiert. In diesem Fall müssen Sie eine der folgenden Aktionen auswählen:

   - **Autonomes Installationspaket erstellen**. Wählen Sie diese Option beispielsweise dann aus, wenn Sie ein autonomes Installationspaket für eine neue Anwendungsversion erstellen und dabei ein autonomes Installationspaket beibehalten möchten, das Sie für eine ältere Anwendungsversion erstellt haben. Das neue autonome Installationspaket wird in einem anderen Ordner abgelegt.

   - **Vorhandenes autonomes Installationspaket verwenden**. Wählen Sie diese Option aus, wenn Sie ein vorhandenes autonomes Installationspaket verwenden möchten. Der Vorgang zur Paket-Erstellung wird nicht gestartet.

   - **Vorhandenes autonomes Installationspaket neu anlegen**. Wählen Sie diese Option aus, wenn Sie ein autonomes Installationspaket für dieselbe Anwendung erneut erstellen möchten. Das autonome Installationspaket wird im selben Ordner abgelegt.

5. Wählen Sie auf der nächsten Seite des Assistenten die Option **Nicht zugeordnete Geräte in folgende Gruppe verschieben** aus und geben Sie eine Administrationsgruppe an, in die das Client-Gerät nach der Installation des Administrationsagenten verschoben werden soll.

   Standardmäßig wird das Gerät in die Gruppe **Verwaltete Geräte** verschoben.

   Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten nicht in eine Administrationsgruppe verschieben möchten, wählen Sie die Option **Geräte nicht verschieben** aus.

6. Nachdem das Erstellen des autonomen Installationspakets abgeschlossen wurde, werden auf der nächsten Seite des Assistenten das Ergebnis für das Erstellen des autonomen Installationspakets und der Pfad des autonomen Pakets angezeigt.

   Mithilfe der Links können Sie:

   - den Ordner mit dem autonomen Installationspaket öffnen.
   - per E-Mail einen Link für das erstellte autonome Installationspaket senden. Um diese Aktion auszuführen, müssen Sie ein E-Mail-Programm starten.
   - Beispiel eines HTML-Codes für die Veröffentlichung des Links auf einer Website. Eine TXT-Datei wird erstellt und die Datei wird in einer Anwendung geöffnet, die mit dem TXT-Format verknüpft ist. In der Datei wird das HTML-Tag <a> mit Attributen angezeigt.

7. Wenn Sie die Liste der autonomen Installationspakete öffnen möchten, aktivieren Sie auf der nächsten Seite des Assistenten die Option **Liste der autonomen Pakete öffnen**.

8. Klicken Sie auf **FERTIGSTELLEN**.

   Der Assistent für das Erstellen eines autonomen Installationspakets wird geschlossen.

Das autonome Installationspaket wird im Unterordner PkgInst des Freigegebenen Ordners des Administrationsservers erstellt und abgelegt. Sie können eine Liste der autonomen Pakete anzeigen. Klicken Sie dazu oberhalb der Liste der Installationspakete auf **Liste der autonomen Pakete anzeigen**.

Erstellen benutzerdefinierter Installationspakete

Mit benutzerdefinierten Installationspaketen können Sie die folgenden Aufgaben ausführen:

- Um ein beliebiges Programm (wie einen Text-Editor) auf einem Client-Gerät zu installieren, beispielsweise mithilfe einer Aufgabe.
- Zum Erstellen eines autonomen Installationspakets.

Ein benutzerdefiniertes Installationspaket ist ein Ordner mit einem Satz von Dateien. Die Quelle, aus der ein benutzerdefiniertes Installationspaket erstellt wird, ist eine *Archivdatei*. Die Archivdatei enthält eine Datei oder mehrere Dateien, die in das benutzerdefinierte Installationspaket aufgenommen werden müssen. Wenn Sie ein benutzerdefiniertes Installationspaket erstellen, können Sie Befehlszeilenparameter angeben, z. B. um das Programm im Silent-Modus zu installieren.

So erstellen Sie ein benutzerdefiniertes Installationspaket:

1. Wählen Sie in der Konsolenstruktur den Punkt **Administrationsserver → Erweitert → Remote-Installation → Installationspakete** aus.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Klicken Sie oberhalb der Liste mit den Installationspaketen auf **Installationspaket erstellen**.

   Der Assistent für das Erstellen eines Installationspakets wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

3. Wählen Sie auf der ersten Seite des Assistenten die Option **Installationspaket für eine angegebene ausführbare Datei erstellen** aus.

4. Geben Sie auf der nächsten Seite des Assistenten den Namen des benutzerdefinierten Installationspakets an.

5. Um ein benutzerdefiniertes Installationspaket zu erstellen, klicken Sie auf der nächsten Seite des Assistenten auf **Durchsuchen** und wählen Sie im Windows-Standardfenster **Öffnen** eine Archivdatei aus, die sich auf den verfügbaren Datenträgern befindet.

   Sie können eine Archiv im zip-, cab-, tar- oder tar.gz-Format hochladen. Es ist nicht möglich, ein Installationspaket aus einer sfx-Datei (selbstextrahierendes Archiv) zu erstellen.

   Die Dateien werden auf den Kaspersky Security Center Administrationsserver heruntergeladen.

6. Geben Sie auf der nächsten Seite des Assistenten die Befehlszeilenparameter einer ausführbaren Datei an.

   Sie können bestimmte Befehlszeilenparameter angeben, um das Programm im Silent-Modus aus dem Installationspaket zu installieren. Die Angabe von Befehlszeilenparametern ist optional.

   Wenn Sie möchten, passen Sie die folgenden Optionen an:

   - **Den gesamten Ordner ins Installationspaket kopieren**

     Wählen Sie diese Option, wenn zur ausführbaren Datei noch zusätzliche Dateien gehören, die für die Programminstallation benötigt werden. Bevor Sie diese Option aktivieren, stellen Sie sicher, dass alle erforderlichen Dateien im selben Ordner gespeichert sind. Wenn diese Option aktiviert ist, fügt das Programm den gesamten Inhalt des Ordners, einschließlich der angegebenen ausführbaren Datei, zum Installationspaket hinzu.

   - **Einstellungen auf die empfohlene Werte der von Kaspersky Security Center erkannte Programme konvertieren**

     Das Programm wird mit den empfohlenen Einstellungen installiert, wenn die Kaspersky-Datenbank Informationen zum entsprechenden Programm enthält.

     Wenn Sie Parameter im Feld **Befehlszeilenparameter der ausführbaren Datei** eingegeben haben, werden sie mit den empfohlenen Einstellungen überschrieben.

     Diese Option ist standardmäßig aktiviert.

     Die Kaspersky-Datenbank wird von den Analysten von Kaspersky erstellt und gepflegt. Für jedes Programm, das zur Datenbank hinzugefügt wird, definieren die Analysten von Kaspersky die optimalen Installationseinstellungen. Die Einstellungen werden so gewählt, dass eine erfolgreiche Remote-Installation des Programms auf einem Client-Gerät gewährleistet wird. Die Datenbank wird automatisch auf dem Administrationsserver aktualisiert, wenn Sie die Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers starten.

   Das Erstellen des benutzerdefinierten Installationspakets wird gestartet.

   Der Assistent meldet, wenn der Vorgang abgeschlossen ist.

   Falls das benutzerdefinierte Installationspaket nicht erstellt wurde, wird eine entsprechende Meldung angezeigt.

7. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

Das von Ihnen erstellte Installationspaket wird in den Unterordner "Pakete" des Freigegebenen Ordners des Administrationsservers heruntergeladen. Nach dem Download erscheint das benutzerdefinierte Installationspaket in der Liste der Installationspakete.

In der Liste der Installationspakete auf dem Administrationsserver können Sie die Eigenschaften der benutzerdefinierten Installationspakete anzeigen und bearbeiten.

Eigenschaften von benutzerdefinierten Installationspaketen anzeigen und bearbeiten

Nachdem Sie ein benutzerdefiniertes Installationspaket erstellt haben, können Sie im Eigenschaftenfenster allgemeine Informationen über das Installationspaket anzeigen und die Installationseinstellungen angeben.

Um die Eigenschaften eines benutzerdefinierten Installationspakets anzuzeigen und zu bearbeiten:

1. Wählen Sie in der Konsolenstruktur den Punkt **Administrationsserver → Erweitert → Remote-Installation → Installationspakete** aus.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Wählen Sie im Kontextmenü eines Installationspakets den Punkt **Eigenschaften** aus.

   Das Eigenschaftenfenster des ausgewählten Installationspakets wird geöffnet.

3. Die folgenden Informationen werden angezeigt:

   - Name des Installationspakets
   - Das im benutzerdefinierten Installationspaket enthaltene Programm
   - Programmversion
   - Erstellungsdatum des Installationspaketes
   - Pfad des benutzerdefinierten Installationspakets auf dem Administrationsserver
   - Starteinstellungen für ausführbare Datei

4. Geben Sie die folgenden Einstellungen an:

   - Name des Installationspakets
   - **Erforderliche Systemkomponenten installieren**

     Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

     Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

     Diese Option ist standardmäßig deaktiviert.

     > Diese Option ist nur verfügbar, wenn die zum Installationspaket hinzugefügte Anwendung von Kaspersky Security Center erkannt wird.

- **Befehlszeilenparameter der ausführbaren Datei**

  Wenn das Programm zusätzliche Parameter für eine Installation im Silent-Modus erfordert, geben Sie diese in diesem Feld an. Weitere Informationen finden Sie in der Dokumentation des Herstellers.

  Sie können auch andere Parameter angeben.

  > Diese Option ist nur für Pakete verfügbar, die nicht auf Basis von Kaspersky-Anwendungen erstellt wurden.

5. Klicken Sie auf **OK** oder **Übernehmen**, um die Änderungen zu speichern.

Die neuen Einstellungen werden gespeichert.

Installationspaket des Administrationsagenten aus dem Programmpaket von Kaspersky Security Center beziehen

Sie können das Installationspaket des Administrationsagenten aus dem Programmpaket von Kaspersky Security Center beziehen, ohne Kaspersky Security Center installieren zu müssen. Anschließend können Sie das Installationspaket verwenden, um den Administrationsagenten auf den Client-Geräten zu installieren.

So beziehen Sie das Installationspaket des Administrationsagenten aus dem Programmpaket von Kaspersky Security Center:

1. Führen Sie die Folgende ausführbare Datei aus dem Programmpaket von Kaspersky Security Center aus: ksc_<Versionsnummer>.<Buildnummer>_full_<Sprache der Lokalisierung>.exe.
2. Klicken Sie im folgenden Fenster auf den Link **Installationspakete entpacken**.
3. Wählen Sie in der Liste der Installationspakete das Kontrollkästchen neben dem Installationspaket für den Administrationsagenten und klicken Sie anschließend auf die Schaltfläche **Weiter**.
4. Klicken Sie bei Bedarf auf die Schaltfläche **Durchsuchen**, um den angezeigten Extraktionsordner für das Installationspaket zu ändern.
5. Klicken Sie auf die Schaltfläche **Entpacken**.

   Das Programm extrahiert das Installationspaket des Administrationsagenten.
6. Wenn der Vorgang abgeschlossen ist, klicken Sie auf die Schaltfläche **Schließen**.

Das Installationspaket des Administrationsagenten wird in den ausgewählten Ordner extrahiert.

Sie können das Installationspaket verwenden, um den Administrationsagenten mit einer der folgenden Methoden zu installieren:

- Lokal, indem Sie die Datei setup.exe aus dem extrahierten Ordner ausführen
- Im Silent-Modus
- Mittels Gruppenrichtlinien von Microsoft Windows

Installationspakete an sekundäre Administrationsserver verteilen

Um Installationspakete auf sekundäre Administrationsserver zu verteilen:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten sekundären Administrationsserver verwaltet.

2. Starten Sie das Erstellen einer Aufgabe zur Verteilung eines Installationspakets auf sekundäre Administrationsserver auf eine der folgenden Arten:

   - Wenn Sie die Aufgabe für sekundäre Administrationsserver einer gewählten Administrationsgruppe erstellen möchten, starten Sie das Erstellen einer Gruppenaufgabe für diese Gruppe.

   - Wenn Sie die Aufgabe für eine Auswahl der sekundären Administrationsserver erstellen möchten, starten Sie das Erstellen einer Aufgabe für eine Reihe von Geräten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** als Aufgabentyp **Installationspakete verteilen** aus.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe zur Verteilung der gewählten Installationspakete auf die gewählten sekundären Administrationsserver erstellt.

3. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe werden die gewählten Installationspakete auf die gewählten sekundären Administrationsserver kopiert.

Installationspakete mithilfe von Verteilungspunkten verteilen

Für die Verteilung von Installationspaketen innerhalb einer Administrationsgruppe können Sie Verteilungspunkte verwenden.

Nach dem Download von Installationspaketen von dem Administrationsserver werden sie durch die Verteilungspunkte automatisch mittels IP-Multicast auf die Client-Geräte verteilt. Der IP-Versand neuer Installationspakete im Rahmen einer Administrationsgruppe erfolgt einmal. Wenn ein Client-Gerät während des Versands vom Unternehmensnetzwerk getrennt wurde, lädt der Administrationsagent des Client-Geräts beim Start der Installationsaufgabe automatisch das benötigte Installationspaket vom Verteilungspunkt.

Daten über die Ergebnisse der Programminstallation an Kaspersky Security Center übertragen

Nachdem ein Installationspaket für das Programm erstellt wurde, können Sie das Installationspaket so anpassen, dass Diagnoseinformationen über die Ergebnisse der Programminstallation an Kaspersky Security Center übertragen werden. Für Installationspakete für Kaspersky-Anwendungen ist die Übertragung von Diagnoseinformationen über die Ergebnisse der Programminstallation standardmäßig angepasst. Es sind keine zusätzlichen Einstellungen erforderlich.

Um die Übertragung von Diagnosedaten über die Ergebnisse der Programminstallation an Kaspersky Security Center zu konfigurieren, gehen Sie wie folgt vor:

1. Wechseln Sie in den Ordner des Installationspakets, das mit Kaspersky Security Center für die ausgewählte Anwendung angelegt wurde. Dieser Ordner liegt im gemeinsamen Ordner, der bei der Installation von Kaspersky Security Center angegeben wurde.

2. Öffnen Sie die Datei mit der Erweiterung kpd oder kud, um sie zu bearbeiten (beispielsweise mit dem Texteditor Notepad von Microsoft Windows).

   Die Datei weist das Format einer gewöhnlichen ini-Konfigurationsdatei auf.

3. Fügen Sie die folgenden Zeilen zu der Datei hinzu:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Dieser Befehl konfiguriert Kaspersky Security Center so, dass es auf das Installationsende des Programms wartet, für welches Installationspaket erstellt wurde, und den Rückgabecode vom Installationsprogramm analysiert. Wenn die Übertragung der Diagnosedaten ausgeschaltet werden muss, setzen Sie den Wert des Schlüssels Wait auf 0.

4. Beschreiben Sie die Rückgabecodes für eine erfolgreiche Installation. Fügen Sie dazu in die Datei die folgenden Zeilen ein:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   > Optionale Schlüssel stehen In eckigen Klammern.

   Zeilensyntax:

   - `<return code>`. Beliebige Zahl, die dem Rückgabecode des Installationsprogramms entspricht. Es können beliebig viele Rückgabecodes eingegeben werden.
   - `<description>`. Textbeschreibung für das Ergebnis der Installation. Die Beschreibung kann fehlen.

5. Beschreiben Sie die Rückgabecodes für eine fehlerhafte Installation. Fügen Sie dazu in die Datei die folgenden Zeilen ein:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   Die Zeilensyntax entspricht der Zeilensyntax für die Rückgabecodes bei einer erfolgreichen Installation.

6. Schließen Sie die kpd- oder kud-Datei, und speichern Sie die vorgenommenen Änderungen.

Die Informationen über die Ergebnisse der Installation des vom Benutzer angegebenen Programms werden in die Ereignisprotokolle von Kaspersky Security Center eingetragen und erscheinen in der Ereignisliste, in den Berichten und in den Ergebnissen der Aufgabenausführung.

Die KSN-Proxy Server-Adresse für Installationspakete festlegen

Wenn sich die Adresse oder die Domäne des Administrationsservers ändert, können Sie die Adresse des KSN-Proxyservers für das Installationspaket festlegen.

So legen Sie die Adresse des KSN-Proxyservers für das Installationspaket fest:

1. Wechseln Sie in der Konsolenstruktur im Ordner **Remote-Installation** mit einem Doppelklick zum Unterordner **Installationspakete**.
2. Wählen Sie im sich öffnenden Menü **Eigenschaften**.
3. Wählen Sie im folgenden Eigenschaftenfenster den Unterabschnitt **Allgemein**.
4. Geben Sie im Unterabschnitt **Allgemein** des Eigenschaftenfensters die Adresse des KSN-Proxyservers ein.

Die Installationspakete verwenden jetzt standardmäßig diese Adresse.

Aktuelle Versionen der Programme downloaden

Kaspersky Security Center ermöglicht den Download von aktuellen Versionen der Programme für Unternehmen, die auf den Kaspersky-Servern zur Verfügung stehen.

Um aktuelle Versionen der Kaspersky-Programme für Unternehmen zu erhalten, gehen Sie wie folgt vor:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des erforderlichen Administrationsservers aus, vergewissern Sie sich, dass die Registerkarte **Überwachung** ausgewählt ist, und klicken Sie im Abschnitt **Bereitstellung** auf den Link **Es stehen neue Versionen für Kaspersky-Programme zur Verfügung**.

     Der Link **Es stehen neue Versionen für Kaspersky-Programme zur Verfügung** ist sichtbar, wenn der Administrationsserver eine neue Version eines Programms für Unternehmen auf dem Kaspersky-Internetserver erkennt.

   - Wählen Sie in der Konsolenstruktur **Erweitert** → **Remote-Installation** → **Installationspakete** aus, klicken Sie im Arbeitsbereich auf **Weitere Aktionen** und wählen Sie in der Dropdown-Liste die Option **Aktuelle Versionen der Kaspersky-Programme anzeigen**.

   Eine Liste mit der aktuellen Version der Kaspersky-Anwendungen wird angezeigt.

2. Sie können die Liste der Kaspersky-Anwendungen filtern, um die Suche nach der gewünschten Anwendung zu vereinfachen.

Klicken Sie im oberen Bereich des Fensters **Aktuelle Programmversionen** auf den Link **Filter**, um die Programmliste nach folgenden Kriterien zu filtern:

- **Komponenten**. Verwenden Sie dieses Kriterium, um die Liste der Kaspersky-Anwendungen nach den Schutzbereichen zu filtern, die in Ihrem Netzwerk verwendet werden.
- **Typ der Software für den Download**. Verwenden Sie dieses Kriterium, um die Liste der Kaspersky-Anwendungen nach Anwendungstyp zu filtern.
- **Folgende Updates und Software anzeigen**. Verwenden Sie dieses Kriterium, um verfügbare Kaspersky-Anwendungen nach bestimmten Versionen zu filtern.
- **Software und Updates in folgenden Sprachen anzeigen**. Verwenden Sie dieses Kriterium, um Kaspersky-Anwendungen mit einer bestimmten Lokalisierungssprache zu filtern.

Drücken Sie auf due Schaltfläche **Übernehmen**, um die ausgewählten Filter anzuwenden.

3. Wählen Sie in der Liste das gewünschte Programm aus.
4. Laden Sie durch Klicken auf den Link in der Zeile **Webadresse des Programmpakets** das Programmpaket herunter.

> Für Updates verwalteter Anwendungen muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center installiert werden. Wenn diese Version höher ist als Ihre aktuelle Version, werden diese Updates zwar angezeigt, können jedoch nicht genehmigt werden. Außerdem können aus solchen Updates keine Installationspakete erstellt werden, bevor Kaspersky Security Center nicht aktualisiert wurde. Sie werden aufgefordert, Ihre Kaspersky Security Center-Instanz auf die erforderliche Mindestversion zu aktualisieren.

Wenn für das gewählte Programm die Schaltfläche **Programme herunterladen und Installationspakete erstellen** angezeigt wird, können Sie auf diese Schaltfläche klicken, damit das Programmpaket heruntergeladen und das Installationspaket automatisch erstellt wird. In diesem Fall wird das Programmpaket durch Kaspersky Security Center auf den Administrationsserver in den gemeinsamen Ordner heruntergeladen, der bei der Installation von Kaspersky Security Center vorgegeben wurde. Das automatisch erstellte Installationspaket wird im Ordner **Remote-Installation** der Konsolenstruktur im Unterordner **Installationspakete** angezeigt.

> Nach dem Schließen des Fensters **Aktuelle Programmversionen**, wird der Link **Es stehen neue Versionen für Kaspersky-Programme zur Verfügung** aus dem Abschnitt **Bereitstellung** entfernt.

Sie können Installationspakete neuer Programmversionen erstellen und mit den erstellten Installationspaketen im Ordner **Remote-Installation** der Konsolenstruktur im Unterordner **Installationspakete** arbeiten.

Das Fenster **Aktuelle Programmversionen** können Sie auch durch Klick auf den Link **Aktuelle Versionen der Kaspersky-Programme anzeigen** im Arbeitsbereich des Ordners **Installationspakete** öffnen.

Ein Windows-Gerät für die Remote-Installation vorbereiten

Die Remote-Installation einer Anwendung auf einem Client-Gerät kann aus den folgenden Gründen fehlerhaft beendet werden:

- Die Aufgabe wurde zuvor schon erfolgreich auf dem Gerät abgeschlossen.

  In diesem Fall muss sie nicht noch einmal ausgeführt werden.

- Beim Aufgabenstart war das Gerät ausgeschaltet.

  In diesem Fall muss das Gerät hochgefahren und die Aufgabe anschließend Neu starten werden.

- Es fehlt eine Verbindung zwischen dem Administrationsserver und dem Administrationsagenten, der auf dem Client-Gerät installiert ist.

  Zur Ursachenforschung können Sie das Tool Remote-Diagnose des Client-Geräts (klactgui) verwenden.

- Wenn der Administrationsagent nicht auf dem Gerät installiert ist, können bei der Remote-Installation des Programms folgende Probleme auftreten:

  - Auf dem Client-Gerät ist **Deaktivieren des einfachen Zugriffs auf Dateien** aktiviert.
  - Auf dem Client-Gerät wird der Dienst Server nicht ausgeführt.
  - Auf dem Client-Gerät sind die Ports geschlossen.
  - Die Berechtigungen des Benutzerkontos, unter dem die Aufgabe ausgeführt wird, reichen nicht aus.

  Um Probleme zu vermeiden, die während der Installation der Anwendung auf einem Client-Gerät ohne installierten Administrationsagent auftreten können, müssen Sie vorgehen, wie hier beschrieben: Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center.

Ursprünglich wurde das Tool "riprep" verwendet, um ein Gerät für die Remote-Installation vorzubereiten. Dies Methode zur Konfiguration von Betriebssystemen gilt nun als veraltet. Die Verwendung des riprep-Tools wird für Betriebssysteme, die neuer sind als Windows XP und Windows Server 2003 R2, nicht empfohlen.

Ein Linux-Gerät vorbereiten und den Administrationsagenten auf einem Linux-Gerät remote installieren

Die Installation des Administrationsagenten umfasst zwei Schritte:

- Vorbereitung eines Linux-Geräts
- Remote-Installation des Administrationsagenten

Vorbereitung eines Linux-Geräts

Um ein Gerät mit dem Betriebssystem Linux für die Remote-Installation des Administrationsagenten vorzubereiten, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie den Administrationsagenten für Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

2. Laden Sie das Installationspaket des Administrationsagenten über die Programmoberfläche oder über die Kaspersky-Website herunter.

3. Stellen Sie sicher, dass auf dem Linux-Zielgerät die folgende Software installiert ist:

   - Sudo (für Ubuntu 10.04 ist Sudo ab Version 1.7.2p1 erforderlich)
   - Perl-Sprachinterpreter ab Version 5.10
   - ps-Tool

4. Testen Sie die Konfiguration des Geräts:

   a. Stellen Sie sicher, dass eine Verbindung zum Gerät über ein Client-Programm mit SSH möglich ist (z. B. PuTTY).

   Wenn Sie keine Verbindung zum Gerät herstellen können, öffnen Sie die Datei `/etc/ssh/sshd_config` und stellen Sie sicher, dass die folgenden Einstellungen die nachstehenden Werte besitzen:

   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

   > Ändern Sie die Datei /etc/ssh/sshd_config nicht, wenn Sie sich problemlos mit dem Gerät verbinden können. Andernfalls kann es zu einem Fehler bei der SSH-Authentifizierung kommen, wenn eine Aufgabe zur Remote-Installation ausgeführt wird.

   Speichern Sie die Datei (bei Bedarf) und starten Sie den SSH-Dienst über den Befehl `sudo service ssh restart` neu.

   b. Stellen Sie sicher, dass auf einem Linux-basierten nicht zugewiesenen Gerät der TCP-Port 22 erreichbar und geöffnet ist. Um den Administrationsagenten für Linux installieren zu können, muss der TCP-Port 22 verfügbar sein.

   c. Deaktivieren Sie das Kennwort der sudo-Abfrage für das Benutzerkonto, das für die Verbindung mit dem Gerät verwendet wird.

   d. Verwenden Sie den Befehl `visudo` in sudo, um die Konfigurationsdatei sudoers zu öffnen.

   Fügen Sie der geöffneten Datei am Ende die folgende Zeile hinzu: `<Benutzername> > ALL = (ALL) NOPASSWD: ALL`. In diesem Fall ist `< Benutzername >` ein Benutzerkonto, das für die Verbindung mit dem Gerät über das SSH-Protokoll verwendet wird. Wenn Sie das Betriebssystem Astra Linux verwenden, fügen Sie am Ende der Datei "/etc/sudoers" die Zeile mit dem folgenden Text an: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   e. Speichern und schließen Sie die Datei sudoers.

   f. Stellen Sie erneut eine Verbindung zum Gerät über SSH her und stellen Sie mithilfe des Befehls `sudo whoami` sicher, dass der Sudo-Dienst kein Kennwort abfragt.

5. Öffnen Sie die Datei `/etc/systemd/logind.conf` file und nehmen Sie folgende Änderungen vor:

   - Geben Sie für die Einstellung "KillUserProcesses" den Wert "no" an: `KillUserProcesses=no`.
   - Geben Sie für die Einstellung "KillExcludeUsers" den Benutzernamen des Kontos an, unter dem die Remote-Installation durchgeführt wird, z. B. `KillExcludeUsers=root`.

   Wenn auf dem Zielgerät Astra Linux ausgeführt wird, fügen Sie die Zeichenfolge export `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` in die Datei `/home/< Benutzername >/.bashrc` ein, wobei `< Benutzername >` für jenes Benutzerkonto steht, das für die Geräteverbindung über SSH verwendet werden soll.

   Um die geänderten Einstellungen zu übernehmen, starten Sie das Linux-Gerät neu oder führen Sie den folgenden Befehl aus:

   ```
   sudo systemctl restart systemd-logind.service
   ```

6. Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

7. Wenn Sie den Administrationsagenten auf Geräten installieren möchten, auf denen das Betriebssystem Astra Linux in der abgeschlossenen Softwareumgebung läuft, führen Sie die zusätzlichen Schritte aus, um die Geräte mit Astra Linux vorzubereiten.

8. Wenn Sie den Administrationsagenten auf Geräten mit den Betriebssystemen RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher installieren möchten, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsagent ordnungsgemäß funktioniert.

Remote-Installation des Administrationsagenten

So installieren Sie den Administrationsagenten remote auf Linux-Geräten:

1. Laden Sie das Installationspaket herunter und erstellen Sie es:

   a. Vergewissern Sie sich vor der Installation des Pakets, dass die Abhängigkeiten für das jeweilige Paket (Programme, Bibliotheken) auf dem Gerät installiert sind.

   Sie können die Abhängigkeiten für jedes Paket selbständig anzeigen, indem Sie die Tools verwenden, die für den Linux- Distributionssatz spezifiziert sind, auf dem das Paket installiert wird. Mit den Informationen über die Tools können Sie sich in der Dokumentation zu Ihrem Betriebssystem vertraut machen.

   b. Verwenden Sie folgende Dateien, um ein Installationspaket für Remote-Installation zu erstellen:

      - klnagent.kpd.
      - akinstall.sh.
      - deb- oder rpm-Paket des Administrationsagenten.

2. Erstellen Sie eine Aufgabe zur Remote-Installation des Programms mit den folgenden Einstellungen:

   - Aktivieren Sie auf der Seite **Einstellungen** des Assistenten für das Erstellen einer Aufgabe das Kontrollkästchen **Durch Ressourcen des Betriebssystems über den Administrationsserver**. Deaktivieren Sie alle anderen Kontrollkästchen.

   - Geben Sie auf der Seite **Benutzerkonto für die Ausführung der Aufgabe auswählen** die Einstellungen des Benutzerkontos an, das für die SSH-Verbindung mit dem Gerät verwendet wird.

3. Starten Sie die Aufgabe zur Remote-Installation des Programms. Verwenden Sie die Option für den Befehl `su`, um die Umgebung beizubehalten: `-m, -p, --preserve-environment`.

Ein Gerät mit SUSE Linux Enterprise Server 15 für die Installation des Administrationsagenten vorbereiten

So installieren Sie den Administrationsagenten auf einem Gerät mit dem Betriebssystem SUSE Linux Enterprise Server 15:

Führen Sie vor der Installation des Administrationsagenten den folgenden Befehl aus:

```
sudo zypper install insserv-compat
```

Dies erlaubt Ihnen die Installation des Pakets insserv-compat, um den Administrationsagenten richtig zu konfigurieren.

Führen Sie den Befehl `rpm -q insserv-compat` aus, um zu prüfen, ob das Paket bereits installiert ist.

Wenn Ihr Netzwerk viele Geräte mit SUSE Linux Enterprise Server 15 umfasst, können Sie das spezielle Programm zum Konfigurieren und Verwalten der Unternehmensinfrastruktur verwenden. Mittels dieses Programms können Sie das Paket insserv-compat automatisch auf allen erforderlichen Geräten gleichzeitig installieren. Sie können beispielsweise Puppet, Ansible, Chef oder Ihr selbsterstelltes Skript verwenden – je nachdem, was für Sie am besten geeignet ist.

Wenn das Gerät nicht über die GPG-Signaturschlüssel für SUSE Linux Enterprise verfügt, wird möglicherweise die folgende Warnung angezeigt: `Package header is not signed!` Um die Warnung zu ignorieren, wählen Sie die Option `i`.

Stellen Sie neben der Installation des Pakets insserv-compat sicher, dass Sie Ihre Linux-Geräte vollständig vorbereitet haben. Anschließend folgt die Bereitstellung und Installation des Administrationsagenten.

Ein Gerät mit dem Betriebssystem macOS für die Remote-Installation des Administrationsagenten vorbereiten

Um ein Gerät mit dem Betriebssystem macOS für die Remote-Installation des Administrationsagenten vorzubereiten, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sudo auf dem macOS-Zielgerät installiert ist.

2. Testen Sie die Konfiguration des Geräts:

   a. Stellen Sie sicher, dass auf dem Client-Gerät der Port 22 geöffnet ist. Um dies zu tun, öffnen Sie in den **Systemeinstellungen** den Bereich **Teilen** und stellen Sie anschließend sicher, dass das Kontrollkästchen **Fernanmeldung** aktiviert ist.

   Sie können sich mittels Secure Shell (SSH) nur über Port 22 mit dem Client-Gerät verbinden. Sie können die Portnummer nicht ändern.

   Sie können den Befehl `ssh <Gerätename>` verwenden, um sich entfernt auf dem macOS-Gerät anzumelden. Im Reiter **Freigaben** können Sie die Option **Auswahl der anmeldeberechtigten Benutzer** verwenden, um die Benutzer festzulegen, denen der Zugriff auf das macOS-Gerät gewährt werden soll.

   b. Deaktivieren Sie das Kennwort der sudo-Abfrage für das Benutzerkonto, das für die Verbindung mit dem Gerät verwendet wird.

   Verwenden Sie den `sudo visudo`-Befehl, um die sudoers-Konfigurationsdatei zu öffnen. Geben Sie in der geöffneten Datei unter dem Eintrag `User privilege specification` folgendes an: `username ALL = (ALL) NOPASSWD: ALL`. In diesem Fall steht `username` für ein Benutzerkonto, das für die Verbindung mit dem Gerät über das SSH-Protokoll verwendet wird.

   c. Speichern und schließen Sie die Datei sudoers.

   d. Stellen Sie erneut eine Verbindung zum Gerät über SSH her und stellen Sie mithilfe des Befehls `sudo whoami` sicher, dass der Sudo-Dienst kein Kennwort abfragt.

3. Laden Sie das Installationspaket herunter und erstellen Sie es:

   a. Laden Sie das Installationspaket des Administrationsagenten mittels einer der folgenden Methoden herunter:

   - Indem Sie in der Konsolenstruktur das Kontextmenü von **Remote-Installation → Installationspakete** öffnen und **Aktuelle Programmversionen anzeigen** wählen, um aus den zur Verfügung stehenden Installationspaketen auszuwählen

   - Indem Sie die benötigte Version des Administrationsagenten von der Website des Technischen Supports unter https://support.kaspersky.com/de herunterladen

   - Durch das Anfordern des Installationspakets von den Spezialisten des Technischen Supports

b. Verwenden Sie folgende Dateien, um ein Installationspaket für Remote-Installation zu erstellen:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Erstellen Sie eine Aufgabe zur Remote-Installation des Programms mit den folgenden Einstellungen:

- Wählen Sie auf der Seite **Einstellungen** des Assistenten für das Erstellen einer Aufgabe das Kontrollkästchen **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Deaktivieren Sie alle anderen Kontrollkästchen.
- Um die Aufgabe auszuführen, geben Sie auf der Seite **Benutzerkonto für die Ausführung der Aufgabe auswählen** die Benutzerkonto-Einstellungen an, die für die Verbindung mit dem Gerät über SSH verwendet werden.

Das Client-Gerät ist zur Remote-Installation des Administrationsagenten über die von Ihnen erstellte entsprechende Aufgabe bereit.

Anwendungen von Kaspersky: Lizenzierung und Aktivierung

Dieser Abschnitt beschreibt die Funktionen von Kaspersky Security Center, die sich auf die Arbeit mit den Lizenzschlüsseln von verwalteten Kaspersky-Anwendungen beziehen.

Kaspersky Security Center ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Anwendungen auf Client-Geräte sowie die Überwachung der Schlüsselverwendung und die Verlängerung der Gültigkeitsdauer der Lizenz.

Beim Hinzufügen eines Lizenzschlüssels über Kaspersky Security Center werden die Lizenzschlüssel-Einstellungen auf dem Administrationsserver gespeichert. Anhand dieser Informationen erstellt die Anwendung einen Bericht über die Nutzung des Lizenzschlüssels und informiert den Administrator über den Ablauf der Gültigkeitsdauer von Lizenzen und eine Überschreitung der in den Lizenzschlüssel-Einstellungen vorgegebenen Lizenzbeschränkungen. Sie können die Einstellungen für Benachrichtigungen über die Nutzung von Lizenzschlüsseln in den Einstellungen des Administrationsservers konfigurieren.

Lizenzierung der verwalteten Programme

Jedes der auf den verwalteten Geräten installierten Kaspersky-Anwendungen muss mit einer Schlüsseldatei oder einem Aktivierungscode lizenziert werden. Eine Schlüsseldatei oder ein Aktivierungscode kann folgendermaßen bereitgestellt werden:

- Mittels automatischer Verteilung
- Mittels Installationspaket der verwalteten Anwendung

- Mittels *Aufgabe zum Hinzufügen eines Lizenzschlüssels* für ein verwaltetes Programm
- Mittels manueller Aktivierung einer verwalteten Anwendung

Sie können mit einer der oben aufgeführten Methoden einen neuen aktiven Lizenzschlüssel oder einen Reserve-Lizenzschlüssel hinzufügen. Kaspersky-Anwendungen verwenden zum aktuellen Zeitpunkt einen aktiven Schlüssel und speichern einen Reserveschlüssel, der nach Ablauf des aktiven Schlüssels angewendet wird. Die Anwendung, für welche Sie einen Lizenzschlüssel hinzufügen, definiert, ob der Schlüssel aktiv oder reserviert ist. Die Definition des Schlüssels hängt nicht von der Methode ab, die Sie zum Hinzufügen des neuen Lizenzschlüssels verwenden.

Mittels automatischer Verteilung

Wenn Sie verschiedene verwaltete Anwendungen verwenden und eine bestimmte Schlüsseldatei oder Aktivierungscode an die Geräte verteilen möchten, verwenden Sie andere Methoden zur Verteilung des Aktivierungscodes oder der Schlüsseldatei.

Kaspersky Security Center erlaubt die automatische Verteilung der vorhandenen Lizenzschlüssel an die Geräte. Angenommen, in der Datenverwaltung des Administrationsservers befinden sich drei Lizenzschlüssel. Sie haben das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** für alle drei Lizenzschlüssel gewählt. Auf den Unternehmensgeräten ist eine Sicherheitsanwendung von Kaspersky installiert, z. B. Kaspersky Endpoint Security für Windows. Ein neues Gerät wurde entdeckt und erfordert die Bereitstellung eines Lizenzschlüssels. Die Anwendung ermittelt, dass für dieses Gerät z. B. zwei Lizenzschlüssel aus dem Speicher geeignet sind: Lizenzschlüssel *Key_1*und Lizenzschlüssel *Key_2*. Einer dieser Lizenzschlüssel wird an das Gerät verteilt. In diesem Fall kann nicht vorausgesagt werden, welcher der beiden Lizenzschlüssel an das Gerät bereitgestellt werden wird, da die automatische Verteilung von Lizenzschlüsseln keinerlei Aktivitäten des Administrators vorsieht.

Bei der Verteilung des Lizenzschlüssels an das Gerät erfolgt eine Zählung aller Geräte, für die dieser Schlüssel gilt. Sie müssen sicherstellen, dass die Anzahl der Geräte, an die der Lizenzschlüssel verteilt wird, die Lizenzbeschränkung nicht überschreitet. Falls die Anzahl der Geräte die Lizenzbeschränkung überschreitet, wird allen Geräten, die nicht durch die Lizenz abgedeckt sind, der Status *Kritisch* zugewiesen.

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- Verwaltungskonsole:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel automatisch verteilen

  oder
- Kaspersky Security Center Web Console:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel automatisch verteilen

Beachten Sie, dass ein automatisch verteilter Lizenzschlüssel in den folgenden Fällen möglicherweise nicht in der Datenverwaltung des virtuellen Administrationsservers angezeigt wird:

- Der Lizenzschlüssel ist nicht für diese Anwendung vorgesehen.
- Der virtuelle Administrationsserver verfügt über keine verwalteten Geräte.
- Der Lizenzschlüssel wird bereits für Geräte verwendet, die unter Verwaltung eines anderen virtuellen Administrationsservers stehen, und die maximale Anzahl an Geräten wurde erreicht.

Hinzufügen einer Schlüsseldatei oder eines Aktivierungscodes zum Installationspaket einer verwalteten Anwendung

Diese Option wird aus Sicherheitsgründen nicht empfohlen. Eine Schlüsseldatei oder ein Aktivierungscode, der zum Installationspaket hinzugefügt wurde, kann kompromittiert werden.

Wenn die Installation der verwalteten Anwendung mithilfe eines Installationspakets erfolgt, können Sie eine Schlüsseldatei oder einen Aktivierungscode im Installationspaket oder in der Richtlinie dieser Anwendung angeben. Der Lizenzschlüssel wird bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver an die verwalteten Geräte verteilt.

Anleitung:

- Verwaltungskonsole:
  - Installationspaket erstellen
  - Programme auf Client-Geräten installieren

  oder
- Kaspersky Security Center Web Console: Lizenzschlüssel zu einem Installationspaket hinzufügen

Verteilung mithilfe der Aufgabe zum Hinzufügen eines Lizenzschlüssels für ein verwaltetes Programm

Wenn Sie die Aufgabe *Lizenzschlüssel hinzufügen* für verwaltete Programme verwenden, können Sie den Lizenzschlüssel auswählen, der an die Geräte verteilt werden soll, und die Geräte auf die von Ihnen bevorzugte Art auswählen, z. B. indem Sie eine Administrationsgruppe oder eine Geräteauswahl wählen.

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- Verwaltungskonsole:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel auf Client-Geräte verteilen

oder

- Kaspersky Security Center Web Console:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel auf Client-Geräte verteilen

Manuelles Hinzufügen des Aktivierungscodes oder der Schlüsseldatei auf den Geräten.

Sie können die installierte Kaspersky-Anwendung lokal mittels der Tools in der Programmoberfläche aktivieren. Weitere Informationen finden Sie in der Dokumentation zum installierten Programm.

Informationen zu verwendeten Lizenzschlüsseln anzeigen

Um sich Informationen über die verwendeten Lizenzschlüssel anzeigen zu lassen,

Wählen Sie in der Konsolenstruktur den Ordner **Lizenzen für Kaspersky-Software** aus.

Im Arbeitsbereich des Ordners wird eine Liste der Lizenzschlüssel angezeigt, die auf den Client-Geräten verwendet werden.

Neben jedem Lizenzschlüssel wird ein Symbol angezeigt, das dem Typ der Schlüsselverwendung entspricht:

-  – Daten über den verwendeten Lizenzschlüssel, die von dem mit dem Administrationsserver verbundenen Client-Gerät empfangen wurden. Die Datei des Lizenzschlüssels wird nicht auf dem Administrationsserver gespeichert.
-  – Der Lizenzschlüssel befindet sich in der Datenverwaltung des Administrationsservers. Die automatische Verteilung dieses Lizenzschlüssels wurde deaktiviert.
-  – Der Lizenzschlüssel befindet sich in der Datenverwaltung des Administrationsservers. Die automatische Verteilung dieses Lizenzschlüssels wurde aktiviert.

Sie können im Eigenschaftenfenster des Client-Geräts im Abschnitt **Programme** Informationen darüber anzeigen lassen, welche Lizenzschlüssel für die Aktivierung eines Programms auf einem Client-Gerät verwendet werden.

Zur Bestimmung der aktuellen Einstellungen für die Lizenzschlüssel des virtuellen Administrationsservers sendet der Administrationsserver mindestens einmal pro Stunde eine Anfrage an die Aktivierungsserver von Kaspersky. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung öffentliche DNS-Server.

Wenn ein Lizenzschlüssel von einem Client-Gerät abgerufen wird, können Sie ihn nicht als Datei exportieren.

Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen

Um einen Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Lizenzen für Kaspersky-Software** aus.
2. Starten Sie die Aufgabe für das Hinzufügen von Lizenzschlüsseln auf eine der folgenden Arten:
   - Wählen Sie im Kontextmenü der Liste der Lizenzschlüssel **Aktivierungscode oder Schlüsseldatei hinzufügen** aus.
   - Klicken Sie im Arbeitsbereich mit der Liste der Lizenzschlüssel auf den Link **Aktivierungscode oder Schlüsseldatei hinzufügen**.
   - Klicken Sie auf die Schaltfläche **Aktivierungscode oder Schlüsseldatei hinzufügen**.

   Der Assistent für das Hinzufügen eines Lizenzschlüssels wird gestartet.
3. Wählen Sie aus, wie Sie den Administrationsserver aktivieren möchten: mit einem Aktivierungscode oder mit einer Schlüsseldatei.
4. Geben Sie Ihren Aktivierungscode oder eine Schlüsseldatei an.
5. Wählen Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aus, wenn Sie sofort einen passenden Lizenzschlüssel in Ihrem Netzwerk verteilen möchten. Wenn Sie diese Option nicht auswählen, können Sie später einen Lizenzschlüssel manuell verteilen.

   Als Ergebnis wird die Schlüsseldatei heruntergeladen und der Assistent für das Hinzufügen eines Lizenzschlüssels ist abgeschlossen. Sie können den hinzugefügten Lizenzschlüssel jetzt in der Liste mit Lizenzen für Kaspersky-Software anzeigen.

Lizenzschlüssel des Administrationsservers entfernen

Um einen Lizenzschlüssel des Administrationsservers zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
2. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers den Abschnitt **Lizenzschlüssel** aus.
3. Entfernen Sie den Lizenzschlüssel, indem Sie auf **Entfernen** klicken.

   Daraufhin wird der Lizenzschlüssel entfernt.

Wenn ein Reserve-Lizenzschlüssel hinzugefügt wurde, wird der Reserve-Lizenzschlüssel automatisch zum aktiven Lizenzschlüssel, nachdem der frühere aktive Lizenzschlüssel entfernt wurde.

Nach dem Entfernen des aktiven Lizenzschlüssels sind die Funktionen Schwachstellen- und Patch-Management und Verwaltung mobiler Geräte auf dem Administrationsserver nicht verfügbar. Sie können den entfernten Lizenzschlüssel erneut hinzufügen oder einen anderen Lizenzschlüssel hinzufügen.

Lizenzschlüssel auf Client-Geräte verteilen

Kaspersky Security Center ermöglicht die Verteilung von Lizenzschlüsseln auf Client-Geräte mit der Aufgabe zur *Verteilung von Lizenzschlüsseln*.

Vor der Verteilung müssen Sie den Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen.

Um einen Lizenzschlüssel auf Client-Geräte zu verteilen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Lizenzen für Kaspersky-Software** aus.
2. Klicken Sie im Arbeitsbereich mit der Liste auf die Schaltfläche **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.

   Der **Assistent für das Erstellen einer Aufgabe zur Programmaktivierung** wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Wählen Sie in der Liste der Programme jenes aus, für das Sie eine Aufgabe erstellen möchten.
4. Fügen Sie im Schritt **Schlüssel hinzufügen** des Assistenten den Lizenzschlüssel mithilfe einer der folgenden Optionen hinzu:

   - Wählen Sie die Option **Aktivierungscode**, um einen Aktivierungscode aus der Datenverwaltung von Kaspersky Security Center hinzuzufügen.

     Klicken Sie auf die Schaltfläche **Auswählen**. Wählen Sie im angezeigten Fenster den Aktivierungscode aus und klicken Sie auf **OK**.

   - Wählen Sie die Option **Schlüsseldatei oder Schlüssel** aus und gehen Sie anschließend wie folgt vor:

     a. Klicken Sie auf die Schaltfläche **Auswählen**.

     b. Wählen Sie im Kontextmenü eine der Optionen aus:

     - **Schlüsseldatei aus einem Ordner**.

       Wählen Sie im angezeigten Fenster die Schlüsseldatei auf Ihrem Gerät aus und klicken Sie auf **Öffnen**.

     - **Schlüssel aus der Kaspersky Security Center-Datenverwaltung**.

       Wählen Sie im angezeigten Fenster den Schlüssel aus der Datenverwaltung von Kaspersky Security Center aus und klicken Sie auf **OK**.
5. Wenn Sie den aktiven Lizenzschlüssel ersetzen möchten, deaktivieren Sie das standardmäßige aktivierte Kontrollkästchen **Als Reserveschlüssel verwenden**.

   Dies kann beispielsweise erforderlich sein, wenn sich die Organisation ändert und der Schlüssel einer anderen Organisation auf dem Gerät benötigt wird; oder wenn der Schlüssel erneut ausgestellt wurde und eine neue Lizenz früher abläuft als die aktuelle Lizenz. Um Fehler zu vermeiden, müssen Sie das Kontrollkästchen **Als Reserveschlüssel verwenden** deaktivieren.

   Weitere Informationen über Probleme, die beim Hinzufügen eines Lizenzschlüssels zu Kaspersky Security Center Windows auftreten können, sowie Möglichkeiten, diese Probleme zu beheben, finden Sie in der Wissensdatenbank von Kaspersky Security Center.

6. Überprüfen Sie die Informationen des Lizenzschlüssels und klicken Sie auf **Weiter**.

7. Wählen Sie in diesem Schritt des Assistenten die Geräte aus, denen Sie die Aufgabe zum Hinzufügen eines Schlüssels zuweisen möchten. Sie können die (bis zu 1.000) Geräte auf eine der folgenden Arten angeben:

   - **Geräte auswählen, die vom Administrationsserver erkannt wurden**. In diesem Fall wird die Aufgabe einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

   - **Geräteadressen manuell angeben oder aus Liste importieren** Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

   - **Aufgabe einer Geräteauswahl zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine vordefinierte Auswahl oder Ihre eigene Auswahl angeben.

   - **Aufgabe einer Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu der zuvor erstellten Administrationsgruppe gehören.

8. Erstellen Sie in dem Schritt **Aufgabenzeitplan anpassen** des Assistenten einen Zeitplan für den Aufgabenstart.

   - **Start nach Zeitplan**:

     - **Einmal**

       Die Aufgabe wird einmal zum angegebenen Datum und zur angegebenen Uhrzeit ausgeführt (standardmäßig entspricht dies dem Tag, an dem die Aufgabe erstellt wurde).

     - **Manuell**

       Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

       Diese Variante ist standardmäßig ausgewählt.

     - **Nach dem Download von Updates in die Datenverwaltung**

       Die Aufgabe wird gestartet, nachdem Updates in die Datenverwaltung heruntergeladen wurden. Sie können diesen Zeitplan beispielsweise zur Suchen nach Suche nach Schwachstellen und erforderlichen Updates verwenden.

     - **Beim Erkennen eines Virenangriffs**

       Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

       - Antiviren-Programme für Workstations und Dateiserver
       - Anti-Virus für Perimeterschutz
       - Anti-Virus für E-Mailsysteme

       Standardmäßig sind alle Anwendungstypen ausgewählt.

       Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

9. Geben Sie im Schritt **Aufgabenname festlegen** des Assistenten den Namen für die Aufgabe an. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

10. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

    Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Aufgaben, die mit dem **Assistent für das Erstellen einer Aufgabe zur Programmaktivierung** erstellt wurden, sind Aufgaben für eine Reihe von Geräten und werden in der Konsolenstruktur im Ordner **Aufgaben** abgelegt.

Außerdem können Sie eine Gruppenaufgabe oder eine lokale Aufgabe zur Verteilung von Lizenzschlüsseln mithilfe des Assistenten für das Erstellen einer Aufgabe für eine Administrationsgruppe und für ein Client-Gerät erstellen.

Lizenzschlüssel automatisch verteilen

Kaspersky Security Center ermöglicht das automatische Verteilen von Lizenzschlüsseln, die sich im Schlüsselspeicher auf dem Administrationsserver befinden, auf die verwalteten Geräte. Das automatische Verteilen von Lizenzschlüsseln wird nicht für Geräte ausgeführt, die sich im Ordner **Nicht zugeordnete Geräte** befinden.

Um einen Lizenzschlüssel automatisch auf die verwalteten Geräte zu verteilen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Lizenzen für Kaspersky-Software** aus.

2. Wählen Sie im Arbeitsbereich des Ordners den Lizenzschlüssel, den Sie automatisch auf die Geräte verteilen möchten.

3. Öffnen Sie das Eigenschaftenfenster des gewählten Lizenzschlüssels auf eine der folgenden Arten:

    - Klicken Sie mit der rechten Maustaste auf den Lizenzschlüssel und wählen Sie **Eigenschaften** aus.

    - Klicken Sie im Informationsfeld des gewählten Lizenzschlüssels auf den Link **Lizenzschlüssel-Einstellungen anzeigen**.

4. Aktivieren Sie im folgenden Eigenschaftenfenster des Lizenzschlüssels das Kontrollkästchen **Automatisch verteilter Lizenzschlüssel**. Schließen Sie das Eigenschaftenfenster des Lizenzschlüssels.

Der Lizenzschlüssel wird automatisch an alle kompatiblen Geräte verteilt.

Die Verteilung des Lizenzschlüssels erfolgt durch den Administrationsagenten. Für das Programm werden keine Aufgaben zur Verteilung eines Lizenzschlüssels erstellt.

Wenn ein Lizenzschlüssel automatisch verteilt wird, werden die Lizenzbeschränkungen für die Anzahl der Geräte berücksichtigt. (Die Beschränkung ist in den Eigenschaften des Lizenzschlüssels festgelegt.) Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Lizenzschlüssels auf Geräte automatisch beendet.

Der virtuelle Administrationsserver verteilt Lizenzschlüssel aus seiner Datenverwaltung und aus der Datenverwaltung des Administrationsservers automatisch. Es wird folgendes Vorgehen empfohlen:

- Verwenden Sie die Aufgabe *Lizenzschlüssel hinzufügen*, um den Lizenzschlüssel auszuwählen, der auf den Geräten verteilt werden soll.

- Vermeiden Sie das Deaktivieren der Option **Automatische Verteilung der Lizenzschlüssel auf die Geräte dieses virtuellen Administrationsservers zulassen** in den Einstellungen des virtuellen Administrationsservers. Andernfalls verteilt der virtuelle Administrationsserver keine Lizenzschlüssel an die Geräte (auch nicht jene Lizenzschlüssel, die sich in der Datenverwaltung des Administrationsservers befinden).

Wenn Sie in dem Eigenschaftenfenster des Lizenzschlüssels das Kontrollkästchen **Automatisch verteilter Lizenzschlüssel** auswählen, wird sofort ein Lizenzschlüssel in Ihrem Netzwerk verteilt. Wenn Sie diese Option nicht auswählen, können Sie später einen Lizenzschlüssel manuell verteilen.

Bericht über die Nutzung von Lizenzschlüsseln erstellen und anzeigen

Um einen Bericht über die Lizenzschlüsselnutzung auf Client-Geräten zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie die Berichtsvorlage **Bericht über die Lizenzschlüsselnutzung** oder erstellen Sie eine neue Berichtsvorlage mit dem gleichen Typ.

Der Arbeitsbereich des Berichts über die Nutzung von Lizenzschlüsseln enthält Informationen über aktive Schlüssel und Reserve-Lizenzschlüssel, die auf den Client-Geräten verwendet werden. Darüber hinaus enthält der Bericht Informationen über Geräte, auf denen Lizenzschlüssel verwendet werden, und über die in den Schlüsseleigenschaften vorgegebenen Einschränkungen.

Informationen zu den Lizenzschlüsseln des Programms anzeigen

Um zu erfahren, welche Lizenzschlüssel von einer Kaspersky-Anwendung verwendet werden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur von Kaspersky Security Center den Knoten **Verwaltete Geräte** aus und wechseln Sie zur Registerkarte **Geräte**.
2. Öffnen Sie mit der rechten Maustaste das Kontextmenü des gewünschten Geräts und wählen Sie den Punkt **Eigenschaften** aus.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts den Abschnitt **Programme** aus.
4. Wählen Sie in der angezeigten Programmliste das Programm aus, dessen Lizenzschlüssel angezeigt werden sollen, und klicken Sie anschließend auf die Schaltfläche **Eigenschaften**.
5. Wählen Sie im nächsten Eigenschaftenfenster des Programms den Abschnitt **Lizenzschlüssel** aus.

   Die Informationen werden im Arbeitsbereich dieses Abschnitts angezeigt.

Eine Lizenzschlüsseldatei exportieren

Wenn Ihr Lizenzschlüssel aus Versehen gelöscht wurde und Sie ihn wiederherstellen möchten, können Sie eine Lizenzschlüsseldatei von einem anderen Administrationsserver exportieren.

Um eine Lizenzschlüsseldatei zu exportieren, benötigen Sie die Berechtigung **Schlüsseldatei exportieren** im Funktionsbereich **Allgemeine Funktionen: Schlüsselverwaltung**.

Wenn ein Lizenzschlüssel von einem Client-Gerät abgerufen wird, können Sie ihn nicht exportieren.

So exportieren Sie einen Lizenzschlüssel:

1. Wählen Sie in der Konsolenstruktur den Ordner **Lizenzen für Kaspersky-Software** aus.
2. Wählen Sie in der Liste den Lizenzschlüssel aus, den Sie als Datei exportieren möchten.
3. Klicken Sie in der angezeigten Infobox auf den Link **Schlüsseldatei exportieren**.
4. Geben Sie im angezeigten Fenster den Pfad des Ordners an, in dem Sie die Lizenzschlüsseldatei speichern möchten, und geben Sie anschließend einen Dateinamen ein. Klicken Sie anschließend auf **Speichern**.

Die Lizenzschlüsseldatei im .key-Format wurde in den ausgewählten Ordner exportiert.

Wenn der Lizenzschlüssel, dessen Datei Sie exportiert haben, der Datenverwaltung des Administrationsservers als Aktivierungscode hinzugefügt wurde und Sie die exportierte Lizenzschlüsseldatei zur Datenverwaltung eines anderen Administrationsservers hinzufügen möchten, müssen Sie diese als Aktivierungscode und nicht als Schlüsseldatei hinzufügen. Andernfalls tritt ein Fehler auf. Sie müssen die exportierte Lizenzschlüsseldatei in einem beliebigen Texteditor öffnen und anschließend den Aktivierungscode kopieren.

Netzwerkschutz konfigurieren

Dieser Abschnitt enthält Informationen über die manuelle Konfiguration von Richtlinien und Aufgaben, über Benutzerrollen und über den Aufbau der Struktur der Administrationsgruppen und der Hierarchie von Aufgaben.

Szenario: Netzwerkschutz konfigurieren

Der Schnellstartassistent erstellt Richtlinien und Aufgaben mit den Standardeinstellungen. Es kann sein, dass diese Einstellungen nicht optimal sind oder in einem Unternehmen als verboten gelten. Deshalb wird empfohlen, die Einstellungen dieser Richtlinien und Aufgaben zu optimieren, und erforderlichenfalls andere Richtlinien und Aufgaben für Ihr Netzwerk zu erstellen.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

- Kaspersky Security Center Administrationsserver installiert haben
- Kaspersky Security Center Web Console installiert haben (optional)
- Das Hauptinstallationsszenario für Kaspersky Security Center abgeschlossen haben
- Der Schnellstartassistent wurde abgeschlossen oder die folgenden Richtlinien und Aufgaben wurden manuell in der Administrationsgruppe **Verwaltete Geräte** erstellt:
  - Richtlinie von Kaspersky Endpoint Security
  - Gruppenaufgabe zum Update von Kaspersky Endpoint Security
  - Richtlinie für den Administrationsagenten
  - Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*

Die Konfiguration des Netzwerkschutzes erfolgt schrittweise:

1. **Einrichtung und Verteilung von Richtlinien und Richtlinienprofilen für Kaspersky-Anwendungen**

   Zur Konfiguration und Verteilung der Einstellungen für auf den verwalteten Geräten installierte Kaspersky-Anwendungen stehen zwei unterschiedliche Methoden der Sicherheitsverwaltung zur Auswahl: die geräteorientierte und die benutzerorientierte Methode. Diese beiden Methoden können auch kombiniert werden. Zur Implementierung einer geräteorientierten Sicherheitsverwaltung können Sie die Werkzeuge nutzen, die von der Microsoft Management Console-basierten Verwaltungskonsole oder von der Kaspersky Security Center Web Console bereitgestellt werden. Die benutzerorientierte Sicherheitsverwaltung kann nur mithilfe der Kaspersky Security Center Web Console erfolgen.

2. **Aufgaben zur Remote-Verwaltung von Kaspersky-Anwendungen konfigurieren**

   Überprüfen Sie die mit dem Schnellstartassistenten erstellten Aufgaben und passen Sie diese bei Bedarf noch feiner an.

   Anleitung:

   - Verwaltungskonsole:
     - Gruppenaufgabe für das Update von Kaspersky Endpoint Security einrichten
     - Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen
   - Kaspersky Security Center Web Console:
     - Gruppenaufgabe für das Update von Kaspersky Endpoint Security einrichten
     - Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates

   Erstellen Sie bei Bedarf zusätzliche Aufgaben, um die auf den Client-Geräten installierten Kaspersky-Anwendungen zu verwalten.

3. **Ereignismenge für Datenbank einschätzen und einschränken**

Informationen über Ereignisse im Betrieb der verwalteten Anwendungen werden vom Client-Gerät übertragen und in der Administrationsserver-Datenbank registriert. Um die Belastung auf den Administrationsserver zu reduzieren, sollten Sie die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, einschätzen und einschränken.

Anleitung:

- Verwaltungskonsole: Beschränkung der maximalen Anzahl der Ereignisse
- Kaspersky Security Center Web Console: Beschränkung der maximalen Anzahl der Ereignisse

Ergebnisse

Nach Abschluss dieses Szenarios wird Ihr Netzwerk dank der Konfiguration von Kaspersky-Anwendungen, den Aufgaben und der vom Administrationsserver empfangenen Ereignissen geschützt sein.

- Die Kaspersky-Anwendungen werden entsprechend den Richtlinien und Richtlinienprofilen konfiguriert.
- Die Anwendungen werden über eine Reihe von Aufgaben verwaltet.
- Die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, ist eingestellt.

Wenn der Netzwerkschutz angepasst ist, können Sie mit der Konfiguration von regelmäßigen Updates für die Kaspersky-Datenbanken und -Programme fortfahren.

Weitere Informationen zum Konfigurieren von automatischen Reaktionen auf Bedrohungen, die durch Kaspersky Sandbox entdeckt wurden, finden Sie in der Online-Hilfe von Kaspersky Sandbox 2.0.

Richtlinien einrichten und verwalten: geräteorientierte Herangehensweise

Nach Abschluss dieses Szenarios werden die Anwendungen gemäß den von Ihnen festgelegten Richtlinien und Richtlinienprofilen auf allen verwalteten Geräten konfiguriert.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie den Kaspersky Security Center Administrationsserver und die Kaspersky Security Center Web Console (optional) installiert haben. Wenn Sie die Kaspersky Security Center Web Console installiert haben, werden Sie womöglich die benutzerorientierte Sicherheitsverwaltung als Alternative oder als zusätzliche Option zur geräteorientierten Herangehensweise in Betracht ziehen.

Schritte

Das Szenario der geräteorientierten Verwaltung der Kaspersky-Anwendungen umfasst die folgenden Schritte:

1. **Anwendungsrichtlinien anpassen**

   Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Anwendungen an, indem Sie für jede Anwendung eine Richtlinie erstellen. Diese Auswahl an Richtlinien wird an die Client-Geräte weitergegeben.

Wenn Sie den Schutz Ihres Netzwerks im Schnellstartassistenten konfigurieren, erstellt Kaspersky Security Center eine Standardrichtlinie für die folgenden Programme:

- Kaspersky Endpoint Security für Windows – für Windows-basierte Client-Geräte
- Kaspersky Endpoint Security für Linux – für Linux-basierte Client-Geräte

Wenn Sie den Konfigurationsvorgang mithilfe dieses Assistenten abgeschlossen haben, müssen Sie keine neue Richtlinie für dieses Programm erstellen. Fahren Sie mit der manuellen Konfiguration der Richtlinie für Kaspersky Endpoint Security fort.

Wenn Sie eine hierarchische Struktur aus mehreren Administrationsservern und/oder Administrationsgruppen haben, erben die sekundären Administrationsserver und die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen und an den sekundären Administrationsserver erzwingen, um Änderungen an den durch die Richtlinie höherer Ebene festgelegten Einstellungen zu verhindern. Wenn Sie möchten, dass nur bestimmte Einstellungen zwangsweise vererbt werden, können Sie diese in der Richtlinie höherer Ebene sperren. Die übrigen, nicht gesperrten Einstellungen können in den Richtlinien niedriger Ebene geändert werden. Dank der erstellten Hierarchie aus Richtlinien können Sie die Geräte in den Administrationsgruppen optimal verwalten.

Anleitung:

- Verwaltungskonsole: Richtlinie erstellen
- Kaspersky Security Center Web Console: Richtlinie erstellen

2. **Richtlinienprofile erstellen (optional)**

Wenn Sie möchten, dass Geräte innerhalb einer Administrationsgruppe verschiedene Richtlinieneinstellungen erhalten, erstellen Sie Richtlinienprofile für diese Geräte. Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von der "zugrundeliegenden" Richtlinie unterscheiden, die auf dem verwalteten Gerät aktiv ist.

Die Verwendung von Bedingungen zur Aktivierung von Profilen erlaubt die Anwendung verschiedener Richtlinienprofile auf Geräte, die sich z. B. in einer bestimmten Einheit oder Sicherheitsgruppe des Active Directory befinden, eine bestimmte Hardware-Konfiguration besitzen oder mit besonderen Tags markiert sind. Verwenden Sie Tags, um Geräte anhand bestimmter Kriterien zu filtern. So können Sie z. B. das Tag *Windows* erstellen, es allen Geräten mit einem Windows-Betriebssystem zuweisen und dieses Tag dann als Bedingung zur Aktivierung eines Richtlinienprofils festlegen. Als Ergebnis werden alle Kaspersky-Anwendungen, die auf Windows-Geräten installiert sind, von ihrem eigenen Richtlinienprofil verwaltet.

Anleitung:

- Verwaltungskonsole:
  - Richtlinienprofil erstellen
  - Regeln für die Aktivierung des Richtlinienprofils erstellen
- Kaspersky Security Center Web Console:
  - Richtlinienprofil erstellen
  - Regeln für die Aktivierung des Richtlinienprofils erstellen

3. **Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergeben**

Standardmäßig wird der Administrationsserver alle 15 Minuten automatisch mit den verwalteten Geräten synchronisiert. Sie können die automatische Synchronisierung umgehen und die Synchronisierung auch manuell mit dem Befehl Synchronisierung erzwingen ausführen. Die Synchronisierung wird auch erzwungen, nachdem Sie eine Richtlinie oder ein Richtlinienprofil erstellt oder geändert haben. Während der Synchronisierung werden neue oder veränderte Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergegeben.

Wenn Sie die Kaspersky Security Center Web Console verwenden, können Sie überprüfen, ob die Richtlinien und Richtlinienprofile an ein bestimmtes Gerät übertragen wurden. Kaspersky Security Center registriert das Datum und die Uhrzeit der Weitergabe in den Eigenschaften des Geräts.

Anleitung:

- Verwaltungskonsole: Erzwungene Synchronisierung
- Kaspersky Security Center Web Console: Erzwungene Synchronisierung

Ergebnisse

Nach Abschluss des geräteorientierten Szenarios werden die Kaspersky-Anwendungen gemäß den festgelegten Einstellungen konfiguriert und mittels Richtlinienhierarchie weitergegeben.

Die konfigurierten Anwendungsrichtlinien und Richtlinienprofile werden automatisch auf neue Geräte angewendet, die zu den Administrationsgruppen hinzugefügt werden.

Geräteorientierte und benutzerorientierte Methode der Sicherheitsverwaltung

Sie können die Sicherheitseinstellungen unter Berücksichtigung der Gerätefunktionen oder der Benutzerrollen verwalten. Die erste Methode wird *geräteorientierte Sicherheitsverwaltung* genannt, die zweite *benutzerorientierte Sicherheitsverwaltung*. Um verschiedene Programmeinstellungen auf verschiedene Geräte anzuwenden, können Sie eine dieser Verwaltungsmethoden oder eine Kombination aus beiden Methoden verwenden. Zur Implementierung einer geräteorientierten Sicherheitsverwaltung können Sie die Werkzeuge nutzen, die von der Microsoft Management Console-basierten Verwaltungskonsole oder von der Kaspersky Security Center Web Console bereitgestellt werden. Die benutzerorientierte Sicherheitsverwaltung kann nur mithilfe der Kaspersky Security Center Web Console erfolgen.

Mit der gerätezentrierten Sicherheitsverwaltung können Sie je nach gerätespezifischen Merkmalen unterschiedliche Einstellungen der Sicherheitsanwendung auf verwaltete Geräte anwenden. So können Sie beispielsweise Geräte, die in verschiedenen Administrationsgruppen zugeordnet sind, mit unterschiedlichen Einstellungen versehen. Sie können die Geräte auch anhand der Verwendung dieser Geräte in Active Directory oder deren Hardware-Spezifikationen unterscheiden.

Die benutzerorientierte Sicherheitsverwaltung ermöglicht es Ihnen, verschiedene Einstellungen der Sicherheitsanwendung auf verschiedene Benutzerrollen anzuwenden. Sie können mehrere Benutzerrollen anlegen, jedem Benutzer eine entsprechende Benutzerrolle zuweisen und verschiedene Anwendungseinstellungen für die Geräte definieren, die sich im Besitz von Benutzern mit unterschiedlichen Rollen befinden. So können Sie zum Beispiel den Geräten von Buchhaltern und den Geräten von Mitarbeitern der Personalabteilung unterschiedliche Anwendungseinstellungen zuweisen. Als Ergebnis erhält bei der benutzerorientierten Sicherheitsverwaltung jede Abteilung – die Buchhaltung und die Personalabteilung – eine eigene Konfiguration der Einstellungen für Kaspersky-Anwendungen. Die Konfiguration der Einstellungen legt fest, welche Anwendungseinstellungen von Benutzern angepasst werden können und welche zwangsweise übernommen und durch den Administrator gesperrt sind.

Bei der benutzerorientierten Sicherheitsverwaltung können Sie einzelnen Benutzern bestimmte Programmeinstellungen zuweisen. Das ist z. B. sinnvoll, wenn ein Mitarbeiter eine besondere Rolle im Unternehmen einnimmt oder wenn Sie Sicherheitsvorfälle überwachen möchten, die auf dem Gerät einer bestimmten Person auftreten. Unter Berücksichtigung der Rolle des Mitarbeiters im Unternehmen können Sie die Berechtigung dieser Person zur Änderung der Programmeinstellungen erweitern oder einschränken. So würden Sie z. B. die Berechtigungen eines Systemadministrators, der Client-Geräte im lokalen Büro verwaltet, erweitern.

Es ist auch eine Kombination der geräteorientierten und der benutzerorientierten Herangehensweise an die Sicherheitsverwaltung möglich. So können Sie zum Beispiel für jede Administrationsgruppe eine bestimmte Programmrichtlinie anpassen und Richtlinienprofile für eine oder mehrere Benutzerrollen Ihres Unternehmens erstellen. In diesem Fall werden die Richtlinien und Richtlinienprofile in der folgenden Reihenfolge angewendet:

1. Es werden Richtlinien angewendet, die für geräteorientierte Sicherheitsverwaltung erstellt wurden.
2. Sie werden mittels Richtlinienprofilen gemäß den Prioritäten der Profile geändert.
3. Die Richtlinien werden von den Richtlinienprofilen geändert, die Benutzerrollen zugewiesen sind.

Richtlinie für Kaspersky Endpoint Security manuell konfigurieren

Dieser Abschnitt enthält Empfehlungen für das Anpassen der Einstellungen der Richtlinie für Kaspersky Endpoint Security, die vom Schnellstartassistenten erstellt wird. Sie können die Einrichtung im Fenster mit den Richtlinieneigenschaften durchführen.

Beachten Sie beim Ändern einer Einstellung, dass Sie über der entsprechenden Einstellung auf die Schaltfläche mit dem "Schloss" klicken müssen, um den Einstellungswert auf der Workstation zu verwenden.

Einstellungen der Richtlinie im Abschnitt "Erweiterter Schutz"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

Im Abschnitt **Erweiterter Schutz** können Sie die Verwendung von Kaspersky Security Network für Kaspersky Endpoint Security für Windows anpassen. Sie können auch die Module von Kaspersky Endpoint Security für Windows anpassen. Dazu zählen "Verhaltensanalyse", "Exploit-Prävention", "Programm-Überwachung" und "Rollback von schädlichen Aktionen".

Es wird empfohlen, im Unterabschnitt **Kaspersky Security Network** die Option **Kaspersky Security Network** zu aktivieren. Diese Option unterstützt Sie bei der Umverteilung und Optimierung des Datenverkehrs im Netzwerk. Wenn die Option **Kaspersky Security Network** deaktiviert ist, können Sie die direkte Verwendung von KSN-Servern aktivieren.

Einstellungen der Richtlinie im Abschnitt "Basisschutz"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

Es wird empfohlen, dass Sie im Abschnitt **Basisschutz** des Eigenschaftsfensters der Richtlinie die zusätzlichen Einstellungen für die Unterabschnitte **Firewall** und **Schutz vor bedrohlichen Dateien** angeben.

Der Unterabschnitt **Firewall** enthält Einstellungen, mit denen Sie die Netzwerkaktivität von Anwendungen auf den Client-Geräten steuern können. Ein Client-Gerät verwendet ein Netzwerk, dem einer der folgenden Statuswerte zugewiesen ist: öffentlich, lokal oder vertrauenswürdig. Je nach Netzwerkstatus kann Kaspersky Endpoint Security die Netzwerkaktivitäten auf einem Gerät zulassen oder verweigern. Wenn Sie Ihrer Organisation ein neues Netzwerk hinzufügen, müssen Sie ihm einen entsprechenden Netzwerkstatus zuweisen. Wenn das Client-Gerät beispielsweise ein Laptop ist, empfehlen wir, dass dieses Gerät das öffentliche oder vertrauenswürdige Netzwerk verwendet, da der Laptop nicht ausschließlich mit dem lokalen Netzwerk verbunden ist. In dem Unterabschnitt **Firewall** können Sie überprüfen, ob Sie die Statuswerte der in Ihrer Organisation verwendeten Netzwerke korrekt zugewiesen haben.

Um die Liste der Netzwerke zu überprüfen, gehen Sie wie folgt vor:

1. Wechseln Sie in den Richtlinieneinstellungen zu Basisschutz → **Firewall**.
2. Klicken Sie im Block **Verfügbare Netzwerke** auf die Schaltfläche **Einstellungen**.
3. Wechseln Sie im angezeigten Fenster **Firewall** zu der Registerkarte **Netzwerke**, um die Liste der Netzwerke anzuzeigen.

In dem Unterabschnitt **Schutz vor bedrohlichen Dateien** können Sie das Untersuchen von Netzlaufwerken deaktivieren. Das Untersuchen von Netzlaufwerken kann eine erhebliche Belastung auf den Netzlaufwerken darstellen. Daher ist es zweckmäßiger, die Untersuchung unmittelbar auf den Dateiservern auszuführen.

Um die Untersuchung von Netzlaufwerken zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie in den Richtlinieneinstellungen zu **Basisschutz** → **Schutz vor bedrohlichen Dateien**.
2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf **Einstellungen**.
3. Deaktivieren Sie neuen Fenster **Schutz vor bedrohlichen Dateien** auf der Registerkarte **Allgemein** das Kontrollkästchen **Alle Netzlaufwerke**.

Einstellungen der Richtlinie im Abschnitt "Allgemeine Einstellungen"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

Es wird empfohlen, dass Sie im Abschnitt **Allgemeine Einstellungen** des Fensters mit den Richtlinieneinstellungen, zusätzliche Einstellungen in den Unterabschnitten **Berichte und Speicher** sowie **Benutzeroberfläche** angeben.

Wechseln Sie im Unterabschnitt **Berichte und Speicher** zum Abschnitt **Datenübertragung an den Administrationsserver**. Das Kontrollkästchen **Über gestartete Programme** gibt an, ob in der Administrationsserver-Datenbank Informationen über alle Versionen aller Module der Apps auf den Geräten im Unternehmensnetzwerk gespeichert werden. Wenn das Kontrollkästchen aktiviert ist, können die gespeicherten Informationen in der Datenbank von Kaspersky Security Center eine erhebliche Größe (mehrere Gigabyte) einnehmen. Deaktivieren Sie das Kontrollkästchen **Über gestartete Programme**, wenn es in der Richtlinie der obersten Ebene aktiviert ist.

Wenn die Verwaltungskonsole den Bedrohungsschutz im Unternehmensnetzwerk zentral verwaltet, deaktivieren Sie die Anzeige der Benutzeroberfläche von Kaspersky Endpoint Security für Windows auf den Workstations. Wechseln Sie dafür im Unterabschnitt **Benutzeroberfläche** zum Abschnitt **Interaktion mit dem Benutzer** und wählen Sie anschließend die Option **Benutzeroberfläche nicht anzeigen** aus.

Um den Passwortschutz auf den Workstations zu aktivieren, wechseln Sie in dem Unterabschnitt **Benutzeroberfläche** zum Abschnitt **Kennwortschutz** und klicken Sie auf die Schaltfläche **Einstellungen**. Aktivieren Sie das anschließend Kontrollkästchen **Kennwortschutz aktivieren**.

Einstellungen der Richtlinie im Abschnitt "Konfiguration von Ereignissen"

Im Abschnitt **Konfiguration von Ereignissen** muss die Speicherung aller Ereignisse auf dem Administrationsserver mit Ausnahme der nachstehenden deaktiviert werden:

- Auf der Registerkarte **Kritisch**:
  - *Autostart des Programms wurde deaktiviert*
  - *Zugriff verweigert*
  - *Programmstart verboten*
  - *Desinfektion nicht möglich*
  - *Endbenutzer-Lizenzvertrag wurde verletzt*
  - *Das Verschlüsselungsmodul konnte nicht geladen werden*
  - *Zwei Aufgaben können nicht gleichzeitig gestartet werden*
  - *Eine aktive Bedrohung wurde gefunden. Die aktive Desinfektion muss gestartet werden*
  - *Netzwerkangriff erkannt*
  - *Nicht alle Komponenten wurden aktualisiert*
  - *Aktivierungsfehler*
  - *Fehler beim Aktivieren des portablen Modus*
  - *Fehler bei Interaktion mit Kaspersky Security Center*
  - *Fehler beim Deaktivieren des portablen Modus*
  - *Fehler beim Ändern der Auswahl der Programmkomponenten*
  - *Fehler bei der Anwendung von Regeln zur Verschlüsselung / Entschlüsselung von Dateien*
  - *Die Richtlinie kann nicht übernommen werden*
  - *Prozess beendet*
  - *Netzwerkaktivität verboten*

- Auf der Registerkarte **Funktionsfehler**: *Ungültige Aufgabeneinstellungen. Einstellungen nicht übernommen*
- Auf der Registerkarte **Warnung**:
  - *Selbstschutz ist deaktiviert*
  - *Ungültiger Reserveschlüssel*
  - *Der Benutzer hat die Verschlüsselungsrichtlinie abgelehnt*
- Auf der Registerkarte **Information**: *Programmstart im Testmodus verboten*

Manuelle Konfiguration der Gruppenaufgabe zum Update von Kaspersky Endpoint Security

Der optimale und empfohlene Zeitplan für die Kaspersky Endpoint Security Version 10 und höher ist **Nach dem Download von Updates in die Datenverwaltung**, wenn das Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert ist.

Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security

Der Schnellstartassistent erstellt die Gruppenaufgabe zur Untersuchung des Geräts. Standardmäßig ist für die Aufgabe der Zeitplan **Donnerstags um 19:00 Uhr starten** mit automatischer Randomisierung ausgewählt und das Kontrollkästchen **Übersprungene Aufgaben starten** ist deaktiviert.

Wenn die Geräte des Unternehmens freitags, beispielsweise um 18:30 deaktiviert werden, bedeutet das, dass die Untersuchungsaufgabe des Geräts niemals ausgeführt wird. Es ist erforderlich, den optimalen Zeitplan dieser Aufgabe ausgehend von den im Unternehmen geltenden Dienstvorschriften zu konfigurieren.

Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen

Der Schnellstartassistent erstellt für den Administrationsagenten die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*. Standardmäßig ist für die Aufgabe der Zeitplan **Dienstag um 19:00 Uhr starten** mit automatischer Randomisierung ausgewählt und das Kontrollkästchen **Übersprungene Aufgaben starten** ist aktiviert.

Wenn die Dienstvorschriften des Unternehmens zu dieser Zeit ein Deaktivieren der Geräte vorsehen, wird die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* nach dem Aktivieren des Geräts (am Mittwochmorgen) ausgeführt. Ein solches Verhalten kann unerwünscht sein, da die Untersuchung auf Schwachstellen eine erhöhte Belastung des Prozessors und des Laufwerkssubsystems des Geräts veranlassen kann. Für einen optimalen Aufgabenzeitplan sollten die im Unternehmen geltenden Regeln und Vorschriften berücksichtigt werden.

Manuelle Konfiguration der Gruppenaufgabe zur Installation von Updates und zum Schließen von Schwachstellen

Der Schnellstartassistent erstellt für den Administrationsagenten die Gruppenaufgabe zur Installation der Updates und zum Schließen von Schwachstellen. Standardmäßig ist der Aufgabenstart täglich um 1:00 Uhr mit zufälliger Verzögerung konfiguriert und die Option **Übersprungene Aufgaben starten** ist deaktiviert.

Wenn die Dienstvorschriften des Unternehmens während der Nacht ein Deaktivieren der Geräte vorsehen, wird die Aufgabe zur Installation der Updates niemals ausgeführt. Es ist erforderlich, den optimalen Zeitplan der Aufgabe zur Untersuchung auf Schwachstellen ausgehend von den im Unternehmen geltenden Dienstvorschriften festzulegen. Ferner muss berücksichtigt werden, dass infolge der Installation der Updates ein Neustart des Geräts erforderlich sein kann.

Maximalen Anzahl an Ereignissen in der Ereignis-Datenverwaltung festlegen

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignis-Datenverwaltung** die Einstellungen für das Speichern der Ereignisse in der Administrationsserver-Datenbank anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Wenn Sie die maximale Anzahl der Ereignisse angeben, berechnet die Anwendung einen ungefähren Wert des für die angegebene Zahl benötigten Speicherplatzes. Sie können diese ungefähre Berechnung verwenden, um zu überprüfen, ob Sie ausreichen freien Platz auf dem Laufwerk haben, um einen Überlauf der Datenbank zu vermeiden. Standardmäßig umfasst die Administrationsserver-Datenbank 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Die Anwendung überprüft die Datenbank alle 10 Minuten. Wenn die Anzahl der Ereignisse den festgelegten Höchstwert plus 10.000 erreicht, löscht die Anwendung die ältesten Ereignisse, sodass nur noch die festgelegte Höchstanzahl von Ereignissen übrig bleibt.

Wenn der Administrationsserver alte Ereignisse löscht, kann er keine neuen Ereignisse in der Datenbank speichern. Während dieser Zeitspanne werden Informationen über abgelehnte Ereignisse in das Kaspersky-Ereignisprotokoll geschrieben. Die neuen Ereignisse werden in die Warteschlange verschoben und dann in der Datenbank gespeichert, nachdem der Löschvorgang abgeschlossen wurde.

Um die Anzahl der Ereignisse, die in der Ereignis-Datenverwaltung des Administrationsservers gespeichert werden können, zu begrenzen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den Administrationsserver und wählen Sie dann **Eigenschaften** aus.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Geben Sie im Arbeitsbereich des Abschnitts **Ereignis-Datenverwaltung Datenverwaltung** die maximale Anzahl der in der Datenbank gespeicherten Ereignisse an.

3. Klicken Sie auf die Schaltfläche **OK**.

Darüber hinaus können Sie die Einstellungen einer beliebigen Aufgabe ändern, um entweder Ereignisse im Zusammenhang mit dem Aufgabenfortschritt oder nur die Ergebnisse der Aufgabenausführung zu speichern. Auf diese Weise reduzieren Sie die Anzahl der Ereignisse in der Datenbank, erhöhen die Ausführungsgeschwindigkeit der Szenarien, die mit der Analyse der Ereignistabelle in der Datenbank verbunden sind, und reduzieren das Risiko der Verdrängung von kritischen Ereignissen durch eine große Anzahl an Ereignissen.

Die maximale Speicherdauer für Informationen über behobenen Schwachstellen festlegen

So legen Sie die maximale Speicherdauer in der Datenbank für die Informationen über bereits behobenen Schwachstellen auf verwalteten Geräten fest:

1. Klicken Sie mit der rechten Maustaste auf den Administrationsserver und wählen Sie dann **Eigenschaften** aus.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Geben Sie im Arbeitsbereich des Abschnitts **Ereignis-Datenverwaltung** die maximale Speicherdauer für Informationen über behobenen Schwachstellen in der Datenbank an.

   Die Speicherdauer beträgt standardmäßig 90 Tage.

3. Klicken Sie auf die Schaltfläche **OK**.

Die maximale Speicherdauer für Informationen über behobene Schwachstellen wird auf die angegebene Anzahl von Tagen begrenzt. Anschließend werden die veralteten Informationen durch die Wartungsaufgabe des Administrationsservers aus der Datenbank gelöscht.

Aufgaben verwalten

Kaspersky Security Center verwaltet die auf Geräten installierten Programme durch das Erstellen und Starten von verschiedenen Aufgaben. Die Aufgaben ermöglichen Installation, Start und Beenden von Programmen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Programm-Module sowie Ausführung anderer Aktionen mit den Programmen.

Die Aufgaben werden in folgende Arten unterteilt:

- *Gruppenaufgaben*. Aufgaben, die auf den Geräten der gewählten Administrationsgruppe ausgeführt werden.
- *Aufgaben des Administrationsservers*. Aufgaben, die auf dem Administrationsserver ausgeführt werden.
- *Aufgaben für eine Reihe von Geräten*. Aufgaben, die auf gewählten Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Administrationsgruppe gehören.
- *Lokale Aufgaben*. Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

Aufgaben für Programme lassen sich nur anlegen, wenn auf dem Administrator-Arbeitsplatz das Verwaltungs-Plug-in für dieses Programm installiert ist.

Zum Erstellen der Liste der (bis zu 1.000) Geräte, für die eine Aufgabe erstellt werden soll, können folgende Methoden angewandt werden:

- Geräte auswählen, die vom Administrationsserver im Netzwerk gefunden wurden.
- Geräteliste manuell erstellen. Als Adresse des Geräts können Sie eine IP-Adresse (oder einen IP-Bereich), den NetBIOS- oder den DNS-Namen verwenden.

- Geräteliste aus einer txt-Datei, die ein Verzeichnis hinzuzufügender Geräte enthält, importieren (jeweils nur eine Adresse pro Zeile).

  Wird die Geräteliste aus der Datei importiert oder manuell erstellt, während die Geräte namentlich identifiziert werden, so werden der Liste nur die Geräte hinzugefügt, deren Daten bereits infolge der Anbindung oder einer Gerätesuche in der Administrationsserver-Datenbank vorhanden sind.

Sie können für jedes Programm eine beliebige Anzahl von Gruppenaufgaben, Aufgaben für eine Reihe von Geräten und lokalen Aufgaben erstellen.

Der Datenaustausch zwischen einem Programm auf dem Gerät und der Datenbank von Kaspersky Security Center erfolgt beim Verbindungsaufbau des Administrationsagenten mit dem Administrationsserver.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt von Aufgaben verfolgen, und Aufgaben kopieren, exportieren, importieren und löschen.

Aufgaben können auf einem Gerät nur dann gestartet werden, wenn das Programm gestartet wurde, für das diese Aufgaben erstellt worden waren. Beim Beenden einer Anwendung wird die Ausführung aller gestarteten Aufgaben abgebrochen.

Die Ergebnisse der Aufgabenausführung werden in den Ereignisprotokollen von Microsoft Windows und von Kaspersky Security Center zentral auf dem Administrationsserver und lokal auf jedem Gerät gespeichert.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Details von Verwaltungsaufgaben für Programme mit Unterstützung von Mandantenfähigkeit

Eine Gruppenaufgabe für eine Anwendung mit Unterstützung von Mandantenfähigkeit wird auf die Anwendung angewendet, abhängig von der Hierarchie der Administrationsserver und Client-Geräte. Der virtuelle Administrationsserver, von dem aus die Aufgabe erstellt wird, muss sich in der gleichen oder einer untergeordneten Administrationsgruppe befinden wie das Client-Gerät, auf dem die Anwendung installiert ist.

Bei Ereignissen, die Ergebnissen einer Aufgabenausführung entsprechen, werden einem Administrator des Anbieters die Informationen über das Gerät angezeigt, auf dem die Aufgabe ausgeführt wird. Stattdessen wird einer Mandantenadministration **Mandantenfähiger Knoten** angezeigt.

Erstellen einer Aufgabe

In der Verwaltungskonsole können Aufgaben unmittelbar im Ordner der Administrationsgruppe, für den die Gruppenaufgabe erstellt wird, und im Arbeitsbereich des Ordners **Aufgaben** erstellt werden.

Um eine Gruppenaufgabe im Ordner einer Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die eine Aufgabe erstellt werden soll.
2. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Aufgaben** aus.
3. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**, um die Erstellung der Aufgabe zu starten.

Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

*Um eine Aufgabe im Arbeitsbereich des Ordners **Aufgaben** zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Klicken Sie auf die Schaltfläche **Abschließen**, um die Erstellung der Aufgabe zu starten.

Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Aufgabe des Administrationsservers erstellen

Der Administrationsserver führt folgende Aufgaben aus:

- Berichte senden
- Download von Updates in die Datenverwaltung des Administrationsservers
- Backup der Daten des Administrationsservers anlegen
- Wartung des Administrationsservers
- Synchronisation von Windows Update durchführen
- Installationspaket auf Basis eines Referenzimages von einem Betriebssystem erstellen
- Remote-Installation eines Programms
- Remote-Deinstallation eines Programms
- Installationspaket verteilen
- Remote-Installation eines Programms auf sekundären Administrationsservern

Auf dem virtuellen Administrationsserver sind nur die Aufgaben zum automatischen Versand von Berichten und zur Erstellung eines Installationspaketes anhand des Betriebssystem-Abbilds eines Mustergeräts verfügbar. In der Datenverwaltung des virtuellen Administrationsservers werden Updates angezeigt, die auf den primären Administrationsserver heruntergeladen wurden. Das Verschieben von Daten des virtuellen Administrationsservers ins Backup wird im Rahmen der Erstellung eines Backups der Daten des primären Administrationsservers ausgeführt.

So erstellen Sie eine Aufgabe des Administrationsservers:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Weisen:
   - Wählen Sie in der Konsolenstruktur aus dem Kontextmenü des Ordners **Aufgaben** den Punkt **Neu** → **Aufgaben** aus.
   - Klicken Sie Arbeitsbereich des Ordners **Aufgaben** auf **Aufgabe erstellen**.

Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Die Aufgaben "Download von Updates in die Datenverwaltung des Administrationsservers", "Windows-Updates synchronisieren", "Wartung des Administrationsservers" und *Backup der Daten des Administrationsservers* lassen sich nur einmal anlegen. Wurden die Aufgaben *Download von Updates in die Datenverwaltung des Administrationsservers*, *Wartung des Administrationsservers*, *Backup der Daten des Administrationsservers erstellen* und *Windows-Updates synchronisieren* bereits für den Administrationsserver erstellt, werden sie im Fenster zur Auswahl eines Aufgabentyps des Assistenten für das Erstellen einer Aufgabe nicht mehr angezeigt.

Aufgabe für eine Reihe von Geräten erstellen

Kaspersky Security Center ermöglicht das Erstellen von Aufgaben für eine Reihe von Geräten nach freier Auswahl. Diese Geräte können zu unterschiedlichen Administrationsgruppen oder zu keiner Administrationsgruppe gehören. Kaspersky Security Center ermöglicht die Ausführung folgender Aufgaben für eine Reihe von Geräten:

- Remote-Installation eines Programms
- Nachricht an Benutzer senden
- Administrationsserver wechseln
- Geräte verwalten
- Updates prüfen
- Installationspakete verteilen
- "Remote-Installation eines Programms auf sekundären Administrationsservern"
- Remote-Deinstallation eines Programms

Um eine Aufgabe für eine Reihe von Geräten zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Weisen:
   - Wählen Sie in der Konsolenstruktur aus dem Kontextmenü des Ordners **Aufgaben** den Punkt **Neu** → **Aufgabe** aus.
   - Klicken Sie Arbeitsbereich des Ordners **Aufgaben** auf **Aufgabe erstellen**.

Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Lokale Aufgaben erstellen

Um eine lokale Aufgabe für ein Gerät zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsbereich der Gruppe, zu welcher das gewünschte Gerät gehört, die Registerkarte **Geräte** aus.
2. Wählen Sie in der Geräteliste auf der Registerkarte **Geräte** das Gerät aus, für das eine lokale Aufgabe erstellt werden soll.
3. Starten Sie den Vorgang zum Erstellen der Aufgabe für das gewählte Gerät auf eine der folgenden Arten:
   - Klicken Sie auf die Schaltfläche **Aktion ausführen** und wählen Sie **Aufgabe erstellen** in der Dropdown-Liste.
   - Klicken Sie auf den Link **Aufgabe erstellen** im Arbeitsbereich für das gewählte Gerät.
   - Verwenden Sie die Geräteeigenschaften auf eine der folgenden Arten:
     a. Wählen Sie im Kontextmenü des Geräts den Punkt **Eigenschaften** aus.
     b. Wählen Sie im folgenden Eigenschaftenfenster des Geräts den Abschnitt **Aufgaben** aus, und klicken Sie auf **Hinzufügen**.

Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Eine ausführliche Beschreibung über das Erstellen und Konfigurieren der lokalen Aufgaben finden Sie in den Handbüchern der betreffenden Kaspersky-Anwendungen.

Vererbte Gruppenaufgabe im Arbeitsbereich der untergeordneten Gruppe darstellen

Um die Anzeige von geerbten Aufgaben für eine untergeordnete Gruppe im Arbeitsbereich zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsbereich der untergeordneten Gruppe die Registerkarte **Aufgaben** aus.
2. Klicken Sie im Arbeitsbereich der Registerkarte **Aufgaben** auf die Schaltfläche **Geerbte Aufgaben anzeigen**.

Daraufhin werden die geerbten Aufgaben mit dem Symbol in der Aufgabenliste angezeigt:

-  – Wenn sie von der Gruppe vererbt wurden, die auf dem primären Administrationsserver erstellt wurde.
-  – Wenn sie von der Gruppe der obersten Ebene vererbt wurden.

Im Modus zum Vererben zur Bearbeitung von vererbten Aufgaben kann nur die Gruppe bearbeitet werden, in der sie erstellt wurden. Die geerbten Aufgaben können in der Gruppe, welche die Aufgaben vererbt, nicht geändert werden.

Geräte vor Ausführung einer Aufgabe automatisch einschalten

Auf ausgeschalteten Geräten werden von Kaspersky Security Center keine Aufgaben ausgeführt. Sie können Kaspersky Security Center so konfigurieren, dass diese Geräte vor dem Aufgabenstart automatisch über die Wake-On-LAN-Funktion eingeschaltet werden.

Um das automatische Einschalten von Geräten vor dem Aufgabenstart zu konfigurieren:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus.
2. Um die Aktionen auf Geräten zu konfigurieren, klicken Sie auf den Link **Erweitert**.
3. Aktivieren Sie im angezeigten Fenster **Erweitert** das Kontrollkästchen **Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren (Min.)** und geben Sie dann den Zeitraum in Minuten an.

Dann verwendet Kaspersky Security Center die Wake-On-LAN-Funktion, um die Geräte zum festgelegten Zeitpunkt vor dem Aufgabenstart einzuschalten und das Betriebssystem zu laden. Nach Abschluss der Aufgabe werden die Geräte automatisch heruntergefahren, falls sich die Gerätebenutzer nicht beim System anmelden. Beachten Sie, dass Kaspersky Security Center nur die Geräte automatisch herunterfährt, die über die Wake-On-LAN-Funktion eingeschaltet wurden.

Kaspersky Security Center kann Betriebssysteme nur auf Geräten automatisch starten, die den Wake-On-LAN-Standard (WOL) unterstützen.

Gerät nach der Ausführung einer Aufgabe automatisch ausschalten

Kaspersky Security Center erlaubt Ihnen, eine Aufgabe so anzupassen, dass nach der Ausführung der Aufgabe diejenigen Geräte, auf denen sie verteilt wird, automatisch ausgeschaltet werden.

Damit Geräte nach der Ausführung der Aufgabe automatisch ausgeschaltet werden, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus.
2. Klicken Sie auf den Link **Erweitert**, um das Fenster zu öffnen, in dem Aktionen mit den Geräten angepasst werden.
3. Aktivieren Sie in dem sich öffnenden Fenster **Erweitert** das Kontrollkästchen **Geräte nach Abschluss der Aufgabe herunterfahren**.

Zeitlimit für Aufgabenausführung festlegen

Um die Zeitdauer der Aufgabenausführung auf Geräten einzuschränken, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus.
2. Klicken Sie auf den Link **Erweitert**, um im folgenden Fenster Aktionen mit den Client-Geräten anzupassen.
3. Aktivieren Sie in dem sich öffnenden Fenster **Erweitert** das Kontrollkästchen **Aufgabe anhalten, wenn sie länger ausgeführt wird als (Min.)** und geben Sie die Zeit in Minuten an.

   Daraufhin wird die Ausführung der Aufgabe von Kaspersky Security Center automatisch abgebrochen, wenn nach Ablauf des angegebenen Zeitraums die Aufgabe nicht beendet wurde.

Aufgaben exportieren

Sie können Gruppenaufgaben und Aufgaben für eine Reihe von Geräten in eine Datei exportieren. Die Aufgaben des Administrationsservers können nicht exportiert werden.

Um eine Aufgabe zu exportieren, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Alle Aufgaben → Exportieren** aus.
2. Geben Sie im folgenden Fenster **Speichern unter** den Namen und Pfad der Datei zum Speichern an.
3. Klicken Sie auf **Speichern**.

Die Rechte der lokalen Administratoren können nicht exportiert werden.

Aufgaben importieren

Sie können Gruppenaufgaben und Aufgaben für eine Reihe von Geräten importieren. Die Aufgaben des Administrationsservers können nicht importiert werden.

Um eine Aufgabe zu importieren, gehen Sie wie folgt vor:

1. Wählen Sie die Liste aus, in welche die Aufgabe importiert werden soll:
   - Wenn Sie die Aufgabe in die Liste mit Gruppenaufgaben importieren möchten, wählen Sie im Arbeitsbereich der gewählten Administrationsgruppe die Registerkarte **Aufgaben** aus.
   - Wenn Sie die Aufgabe in die Liste mit Aufgaben für eine Reihe von Geräten importieren möchten, wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Wählen Sie eine der folgenden Methoden für den Import der Aufgabe aus:
   - Wählen Sie im Kontextmenü der Aufgabenliste **Alle Aufgaben** → **Importieren** aus.
   - Klicken Sie auf den Link **Aufgabe aus Datei importieren** im Block zur Verwaltung der Aufgabenliste.
3. Geben Sie im folgenden Fenster den Pfad zur Datei an, aus der Sie die Aufgabe importieren wollen.
4. Klicken Sie auf **Öffnen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste angezeigt.

Wenn die neu importierte Aufgabe einen identischen Namen wie eine bereits vorhandene Aufgabe hat, wird der Name der importierten Aufgabe um den Index **(<nächste Sequenznummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Aufgaben konvertieren

Kaspersky Security Center ermöglicht es, die Aufgaben vorheriger Versionen der Kaspersky-Anwendungen in die Aufgaben aktueller Programmversionen zu konvertieren.

Die Konvertierung von Aufgaben ist für die folgenden Programme möglich:

- Kaspersky Anti-Virus 6.0 für Windows Workstation MP4
- Kaspersky Endpoint Security 8 für Windows
- Kaspersky Endpoint Security 10 für Windows

Um Aufgaben konvertieren zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus, für den Aufgaben konvertiert werden sollen.

2. Wählen Sie im Kontextmenü des Administrationsservers den Punkt **Alle Aufgaben → Assistent für das Massenkonvertieren von Richtlinien und Aufgaben**.

   Daraufhin wird der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben gestartet. Folgen Sie den Anweisungen des Assistenten.

Nach Fertigstellung des Assistenten werden neue Aufgaben erstellt, welche die Einstellungen vorheriger Programmversionen verwenden.

Aufgaben manuell starten und beenden

Sie können die Aufgaben auf zwei Arten starten und beenden: mithilfe des Kontextmenüs der Aufgabe und im Eigenschaftenfenster des Client-Geräts, für das diese Aufgabe bestimmt wurde.

Die Gruppenaufgaben können mithilfe des Kontextmenüs des Geräts von **Benutzern, die zur Gruppe KLAdmins** gehören, gestartet werden.

Gehen Sie wie folgt vor, um eine Aufgabe vom Kontextmenü oder vom Eigenschaftenfenster der Aufgabe aus zu starten bzw. zu beenden:

1. Wählen Sie in der Aufgabenliste die Aufgabe aus.

2. Starten Sie oder beenden die Aufgabe auf eine der folgenden Arten:

   - Durch Auswählen von **Starten** oder **Beenden** im Kontextmenü der Aufgabe.

   - Durch Klicken auf **Starten** oder **Beenden** im Abschnitt **Allgemein** des Eigenschaftenfensters der Aufgabe.

Gehen Sie wie folgt vor, um eine Aufgabe vom Kontextmenü oder vom Eigenschaftenfenster des Client-Geräts aus zu starten bzw. zu beenden:

1. In der Liste der Geräte wählen Sie das Gerät aus.

2. Starten Sie oder beenden die Aufgabe auf eine der folgenden Weisen:

   - Durch Auswählen von **Alle Aufgaben → Aufgabe starten** im Kontextmenü des Geräts. Wählen Sie in der Aufgabenliste die betreffende Aufgabe.

     Die Liste der Geräte, für welche die Aufgabe bestimmt wurde, wird durch das gewählte Gerät ersetzt. Die Aufgabe wird gestartet.

   - Durch Anklicken der Start- () oder Stop-Schaltfläche () im Abschnitt **Aufgaben** des Fensters mit den Geräteeigenschaften.

Aufgaben manuell fortsetzen und anhalten

Um die Ausführung einer Aufgabe anzuhalten oder fortzusetzen, gehen Sie wie folgt vor:

1. Wählen Sie in der Aufgabenliste die Aufgabe aus.
2. Halten Sie die Aufgabe an oder setzen Sie die Ausführung der Aufgabe auf eine der folgenden Arten fort:
   - Durch Auswählen von **Anhalten** oder **Fortsetzen** im Kontextmenü der Aufgabe.
   - Klicken Sie im Abschnitt **Allgemein** im Eigenschaftenfenster der Aufgabe auf **Anhalten** oder **Fortsetzen**.

Aufgabenausführung überwachen

Um die Aufgabenausführung zu überwachen, gehen Sie wie folgt vor:

Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.

Im mittleren Fensterbereich des Abschnitts **Allgemein** werden Informationen über den aktuellen Status der Aufgabe angezeigt.

Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen

Kaspersky Security Center erlaubt Ihnen, die Ausführungsergebnisse für Gruppenaufgaben, Aufgaben für eine Reihe von Geräten und Aufgaben des Administrationsservers anzuzeigen.

Um sich die Ergebnisse der Aufgabenausführung anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.
2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.

So zeigen sie die Ergebnisse der Aufgabenausführung für einen sekundären Administrationsserver an:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.
2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.
3. Klicken Sie auf **Statistiken von sekundären Servern**.
4. Wählen Sie den sekundären Server aus, für den Sie das Fenster **Ergebnisse der Aufgabenausführung** anzeigen möchten.

Filter für die Informationen über die Ergebnisse der Aufgabenausführung konfigurieren

Kaspersky Security Center erlaubt Ihnen, Informationen über die Ausführungsergebnisse von Gruppenaufgaben, Aufgaben für eine Reihe von Geräten und Aufgaben des Administrationsservers zu filtern. Für die lokalen Aufgaben ist der Filter nicht verfügbar.

Um den Filter für die Informationen über die Ergebnisse der Aufgabenausführung einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.
2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.

   In der Tabelle im oberen Bereich des Fensters wird die Liste aller Geräte angezeigt, denen die Aufgabe zugewiesen wurde. In der Tabelle im unteren Bereich des Fensters werden die Ergebnisse der Aufgabenausführung des ausgewählten Geräts angezeigt:
3. Öffnen Sie in der gewünschten Tabelle mithilfe der rechten Maustaste das Kontextmenü und wählen Sie darin den Punkt **Filter**.
4. Konfigurieren Sie im folgenden Fenster **Filter anwenden** in den Abschnitten **Ereignisse**, **Geräte** und **Uhrzeit** die Einstellungen für den Filter. Klicken Sie auf die Schaltfläche **OK**.

Im Fenster **Ergebnisse der Aufgabenausführung** werden jetzt die Informationen angezeigt, die den eingegebenen Filtereinstellungen entsprechen.

Ändern der Aufgabe Rollback der Änderungen

Um eine Aufgabe zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Aufgaben** die Aufgabe aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Aufgabe.
3. Nehmen Sie die notwendigen Änderungen vor.

   Im Abschnitt **Ausschlüsse vom Gültigkeitsbereich der Aufgabe** kann die Liste der Untergruppen, auf die sich die Aufgabe nicht erstrecken soll, angepasst werden.
4. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die Änderungen der Aufgabe werden in den Eigenschaften der Aufgabe, im Abschnitt **Revisionsverlauf** gespeichert.

Notfalls können Sie die Änderungen der Aufgabe zurücksetzen.

Um die Änderungen einer Aufgabe zurückzusetzen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Wählen Sie die Aufgabe, deren Änderungen zurückgesetzt werden sollen, aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Aufgabe.
3. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Revisionsverlauf** aus.
4. Wählen Sie in der Liste mit den Aufgabenrevisionen die Nummer der Revision aus, deren Änderungen zurückgesetzt werden sollen.
5. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Rollback**.

Vergleich von Aufgaben

Sie können Aufgaben desselben Typs vergleichen: man kann also beispielsweise zwei Aufgaben zur Schadsoftware-Untersuchung vergleichen, aber man kann keine Aufgaben zur Schadsoftware-Untersuchung mit einer Aufgabe zur Installation von Updates vergleichen. Als Ergebnis des Vergleiches der Aufgaben erhalten Sie einen Bericht, in dem angezeigt wird, welche Einstellungen der Aufgaben übereinstimmen, und welche sich unterscheiden. Sie können den Bericht über den Vergleich der Aufgaben ausdrucken oder in einer Datei speichern. Ein Vergleich von Aufgaben kann dann erforderlich sein, wenn es für verschiedene Abteilungen eines Unternehmens verschiedene Aufgaben desselben Typs gibt. Zum Beispiel gibt es für die Buchhaltung eine Aufgabe, in der nur die lokalen Gerätelaufwerke auf Schadsoftware untersucht werden. Zusätzlich gibt es eine Aufgabe für die Verkaufsabteilung, deren Mitarbeiter mit den Kunden korrespondieren, in der sowohl die lokalen Laufwerke, als auch die E-Mails untersucht werden. Um solche Unterschiede rasch zu erkennen, müssen nicht alle Einstellungen der Aufgabe überprüft werden, es genügt, einen Vergleich der Aufgaben auszuführen.

Ein Vergleich ist nur für die Aufgaben desselben Typs möglich.

Die Aufgaben können nur paarweise verglichen werden.

Sie können die Aufgaben auf zwei Arten vergleichen: eine Aufgabe auswählen und mit einer anderen vergleichen oder zwei Aufgaben aus der Liste der Aufgaben vergleichen.

Um eine Aufgabe auszuwählen und mit einer anderen zu vergleichen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Aufgaben** die Aufgabe aus, die mit einer anderen Aufgabe verglichen werden soll.
3. Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Alle Aufgaben → Mit anderer Aufgabe vergleichen** aus.
4. Wählen Sie im Fenster **Aufgabe auswählen** die Aufgabe zum Vergleich aus.
5. Klicken Sie auf die Schaltfläche **OK**.

Es wird ein Bericht über den Vergleich zweier Aufgaben im html-Format angezeigt.

Um zwei Aufgaben aus der Liste der Aufgaben zu vergleichen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Wählen Sie im Ordner **Aufgaben** in der Liste der Aufgaben mithilfe der Tasten **Umschalt** oder **Strg** zwei Aufgaben desselben Typs aus.
3. Wählen Sie im Kontextmenü den Punkt **Vergleichen** aus.

   Es wird ein Bericht über den Vergleich der ausgewählten Aufgaben im html-Format angezeigt.

Beim Vergleich von Aufgaben werden im Bericht des Aufgabenvergleichs die Zeichen ****** angezeigt, falls sich die verwendeten Kennwörter unterscheiden.

Wenn das Kennwort in den Eigenschaften einer Aufgabe geändert wurde, werden im Bericht des Vergleichs der Aufgabenrevisionen die Zeichen ****** angezeigt.

Die Benutzerkonten für den Aufgabenstart

Sie können ein Benutzerkonto festlegen, unter dem eine Aufgabe gestartet werden soll.

Zum Beispiel sind zur Ausführung von Aufgaben zur Untersuchung auf Befehl Zugriffsrechte auf das zu untersuchende Objekt erforderlich, und zur Ausführung von Update-Aufgaben Zugriffsrechte für den autorisierten Proxyserver-Benutzer. Das Festlegen eines Benutzerkontos für den Aufgabenstart ermöglicht es, Fehler bei der Ausführung der Aufgabe zur Untersuchung auf Befehl und der Update-Aufgabe zu vermeiden, wenn der Benutzer, der eine Aufgabe gestartet hat, nicht über die entsprechenden Zugriffsrechte verfügt.

In den Aufgaben zur Remote-Installation/-Deinstallation des Programms wird ein Benutzerkonto für den Download der (de)installationsrelevanten Dateien auf die Client-Geräte verwendet, wenn auf dem Gerät der Administrationsagent nicht installiert oder nicht verfügbar ist. Beim installierten und verfügbaren Administrationsagenten wird das Benutzerkonto verwendet, wenn die Bereitstellung der Dateien gemäß den Aufgabeneinstellungen nur mit Microsoft Windows-Funktionen aus dem freigegebenen Ordner erfolgt. In diesem Fall muss das Benutzerkonto auf dem Client-Gerät über folgende Berechtigungen verfügen:

- Recht auf Remote-Start von Anwendungen
- Rechte für die Ressource "Admin$"
- Recht *Als Dienst anmelden*

Wenn der Administrationsagent die Dateien für Client-Geräte bereitstellt, wird das Benutzerkonto nicht verwendet. Alle Kopiervorgänge und die Installation der Dateien erledigt der **Administrationsagent** unter dem **Konto "LocalSystem"**.

Verlauf der Aufgabenausführung exportieren

Wenn bei einer Aufgabe Probleme auftreten, müssen Sie möglicherweise die Ursachen dafür herausfinden. Um dies zu tun, können Sie den Verlauf der Aufgabenausführung exportieren und anschließend weiterführend analysieren.

So exportieren Sie den Verlauf der Aufgabenausführung:

1. Legen Sie in einem Verzeichnis auf Ihrem Gerät eine leere txt-Datei an.

   Der Verlauf der Aufgabenausführung wird in diese Datei exportiert.

2. Öffnen Sie das Fenster mit den Aufgabenergebnissen.

3. Wählen Sie im oberen Teil des Fensters mit den Aufgabenergebnissen das Gerät aus, bei dem die Probleme auftreten.

4. Im unteren Teil des Fensters mit den Aufgabenergebnissen wird der Ausführungsverlauf für das ausgewählte Gerät angezeigt. Wählen Sie hier mindestens ein Ereignis aus.

   Mit der **Umschalt**- oder **Strg**-Taste können Sie mehrere Ereignisse auszuwählen.

5. Klicken Sie mit der rechten Maustaste auf die Ereignisauswahl, um das Kontextmenü zu öffnen und und **Exportieren** auszuwählen.

   Daraufhin wird der Assistent für den Ereignis-Export gestartet.

6. Klicken Sie im Schritt **Exportdatei** des Assistenten auf die Schaltfläche **Durchsuchen** und wählen Sie anschließend die txt-Datei aus, die Sie für den Export des Verlaufs der Aufgabenausführung angelegt haben.

   Wenn Sie nur die ausgewählten Ereignisse exportieren möchten, aktivieren Sie die Option **Nur ausgewählte Ereignisse exportieren**.

   Wenn Sie den gesamten Verlauf der Aufgabenausführung (alle Ereignisse) exportieren möchten, muss die Option **Nur ausgewählte Ereignisse exportieren** deaktiviert werden.

7. Klicken Sie auf die Schaltfläche **Weiter**.

8. Aktivieren Sie im Schritt **Exportformat** des Assistenten eine der folgenden Optionen:

   - **Als tabulatorgetrennten Text im UNICODE-Format exportieren**

     Aktivieren Sie diese Option, wenn die exportierten Daten Sonderzeichen und Symbole aus mehreren Sprachen enthalten und Sie sicherstellen müssen, dass beim Öffnen der txt-Datei mit den exportierten Daten in verschiedensten Anwendungen alle Zeichen korrekt angezeigt werden.

   - **Als tabulatorgetrennten Text exportieren**

     Aktivieren Sie diese Option, wenn Ihnen die Kompatibilität mit älteren Systemen oder mit Anwendungen, die möglicherweise kein Unicode unterstützen, wichtig ist.

9. Klicken Sie auf die Schaltfläche **Weiter**, um den Assistenten zu beenden.

Der Verlauf der Aufgabenausführung wird in die ausgewählte txt-Datei exportiert.

Assistent zum Ändern der Aufgabenkennwörter

Für eine nicht lokale Aufgabe können Sie ein Benutzerkonto angeben, unter dem die Aufgabe ausgeführt werden soll. Sie können das Benutzerkonto bei der Aufgabenerstellung oder in den Eigenschaften einer vorhandenen Aufgabe angeben. Wenn das angegebene Benutzerkonto den Sicherheitsvorschriften des Unternehmens unterliegt, müssen Sie das Benutzerkonto-Kennwort möglicherweise von Zeit zu Zeit ändern. Wenn das Benutzerkonto-Kennwort abläuft und Sie ein neues festlegen, müssen Sie das neue gültige Kennwort in den Aufgabeneigenschaften angeben, damit die Aufgaben korrekt starten können.

Mit dem Assistenten zum Ändern der Aufgabenkennwörter können Sie das alte Kennwort in allen Aufgaben, in denen das Benutzerkonto angegeben ist, automatisch durch das neue Kennwort ersetzen. Alternativ können Sie dies manuell in den Eigenschaften der einzelnen Aufgaben tun.

Um den Assistenten zum Ändern der Aufgabenkennwörter zu starten:

1. Wählen Sie in der Konsolenstruktur den Knoten **Aufgaben** aus.
2. Wählen Sie im Kontextmenü des Knotens **Assistent zum Ändern der Aufgabenkennwörter** aus.

   Folgen Sie den Anweisungen des Assistenten.

Schritt 1. Eingeben der Anmeldedaten

Geben Sie in den Feldern **Benutzerkonto** und **Kennwort** die neuen Anmeldedaten an, die momentan in Ihrem System gültig sind (z. B. in Active Directory). Wenn Sie zum nächsten Schritt des Assistenten wechseln, überprüft Kaspersky Security Center, ob der angegebene Benutzerkonto-Name mit dem Benutzerkonto-Namen in den Eigenschaften der einzelnen nicht lokalen Aufgaben übereinstimmt. Stimmen die Benutzerkonto-Namen überein, so wird das Kennwort in den Aufgabeneigenschaften automatisch durch das neue ersetzt.

Wenn Sie das Feld **Altes Kennwort (optional)** ausfüllen, ersetzt Kaspersky Security Center das Kennwort nur für jene Aufgaben, in denen sowohl der Benutzerkonto-Name als auch das alte Kennwort gefunden werden. Das Ersetzen erfolgt automatisch. In allen übrigen Fällen müssen Sie eine Aktion auswählen, die beim nächsten Schritt des Assistenten ausgeführt werden soll.

Schritt 2. Auswählen eines Vorgangs

Wenn Sie beim ersten Schritt des Assistenten das alte Kennwort nicht angegeben haben oder das angegebene alte Kennwort nicht mit den Kennwörtern in den Aufgaben übereinstimmt, müssen Sie eine Aktion auswählen, die für die gefundenen Aufgaben ausgeführt werden soll.

Entscheiden Sie für jede Aufgabe, die den Status *Genehmigung benötigt* besitzt, ob Sie das Kennwort in den Aufgabeneigenschaften löschen oder durch das neue Kennwort ersetzen möchten. Wenn Sie das Löschen des Kennworts auswählen, wird die Aufgabe so geändert, dass sie unter dem Standard-Benutzerkonto ausgeführt wird.

Schritt 3. Anzeigen der Ergebnisse

Zeigen Sie beim letzten Schritt des Assistenten die Ergebnisse die einzelnen gefundenen Aufgaben an. Klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.

Hierarchie der Administrationsgruppen erstellen, die dem virtuellen Administrationsserver untergeordnet sind

Nachdem der virtuelle Administrationsserver erstellt wurde, enthält er nur die Administrationsgruppe **Verwaltete Geräte**.

Der Vorgang zum Erstellen einer Hierarchie der dem virtuellen Administrationsserver untergeordneten Administrationsgruppen stimmt mit dem Vorgang zum Erstellen einer Hierarchie der Administrationsgruppen überein, die dem physikalischen Administrationsserver untergeordnet sind.

Den Administrationsgruppen, die dem virtuellen Administrationsserver untergeordnet sind, können Sie keine sekundären und virtuellen Administrationsserver hinzufügen. Dies ist mit den Beschränkungen von virtuellen Administrationsservern verbunden.

Richtlinien und Richtlinienprofile

In Kaspersky Security Center Web Console können Sie Richtlinien für Kaspersky-Anwendungen erstellen. In diesem Abschnitt werden Richtlinien und Richtlinienprofile beschrieben, und Sie erhalten Anweisungen für deren Erstellung und Änderung.

Richtlinienhierarchie, Verwendung von Richtlinienprofilen

Dieser Abschnitt enthält Informationen über Besonderheiten der Anwendung von Richtlinien auf Geräte in Administrationsgruppen. Dieser Abschnitt enthält auch Informationen zu Richtlinienprofilen.

Hierarchie der Richtlinien

In Kaspersky Security Center sind Richtlinien für die Angabe eines identischen Satzes von Einstellungen auf mehreren Geräten vorgesehen. Beispielsweise betrifft der Gültigkeitsbereich der Richtlinie des Programms P, die für die Administrationsgruppe G bestimmt ist, die verwalteten Geräte mit dem installierten Programm P in der Administrationsgruppe G und allen ihren Untergruppen, mit Ausnahme jener Untergruppen, in deren Eigenschaften das Kontrollkästchen **Aus übergeordneter Gruppe erben** deaktiviert ist.

Eine Richtlinie unterscheidet sich von den lokalen Einstellungen durch das Vorhandensein von Schloss-Symbolen ( ) neben den in ihr enthaltenen Einstellungen. Ein aktiviertes "Schloss" in den Richtlinieneigenschaften bedeutet, dass die entsprechende Einstellung (bzw. die Einstellungsgruppe) erstens beim Erstellen der wirksamen Einstellungen verwendet werden soll, und zweitens auf die niedrigere Richtlinie angewendet werden soll.

Das Erstellen der auf dem Gerät geltenden Einstellungen kann auf folgende Weise realisiert werden: Aus der Richtlinie die Werte der Einstellungen mit nicht aktiviertem Schloss übernehmen und die Werte der lokalen Einstellungen darüber speichern. Dann werden über die erhaltenen Werte die aus der Richtlinie übernommenen Werte der Einstellungen mit aktiviertem Schloss gespeichert.

Die Richtlinien ein und desselben Programms beeinflussen einander gegenseitig gemäß der Hierarchie der Administrationsgruppen: die Einstellungen mit dem aktivierten Schloss aus der höher liegenden Richtlinien überschreiben die gleichnamigen Einstellungen aus der niedriger liegenden Richtlinie.

Es existiert eine besondere Art von Richtlinie, nämlich die Richtlinie für mobile Benutzer. Diese Richtlinie tritt auf einem Gerät in Kraft, wenn das Gerät in den Modus für mobile Benutzer wechselt. Mobile Richtlinien gelten gemäß der Hierarchie der Administrationsgruppen nicht auf andere Richtlinien.

Richtlinienprofile

Die Anwendung der Richtlinien auf den Geräten nur aufgrund der Hierarchie der Administrationsgruppen ist in vielen Fällen ungeeignet. Es kann erforderlich werden, in verschiedenen Administrationsgruppen mehrere Kopien einer Richtlinie zu erstellen, die sich ein bis zwei Einstellungen unterscheiden, und im Folgenden den Inhalt dieser Richtlinien manuell zu synchronisieren.

Um Ihnen zu helfen, solche Probleme zu vermeiden, unterstützt Kaspersky Security Center *Richtlinienprofile*. Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von "zugrundeliegenden" Richtlinie unterscheiden, die auf dem Client-Gerät (Computer, mobiles Gerät) gilt. Bei der Aktivierung des Profils werden die Einstellungen der bis zur Aktivierung des Profils auf dem Gerät geltenden Richtlinie geändert. Diese Einstellungen nehmen die im Profil festgelegten Werte an.

Richtlinienprofile haben derzeit folgende Einschränkungen:

- Die Richtlinie darf nicht mehr als 100 Profile enthalten.
- Ein Richtlinienprofil kann keine anderen Profile enthalten.
- Ein Richtlinienprofil darf keine Benachrichtigungseinstellungen enthalten.

Zusammensetzung des Profils

Ein Richtlinienprofil enthält die folgenden Bestandteile:

- Name. Profile mit identischen Namen wirken sich auf einander gemäß der Hierarchie der Administrationsgruppen mit den allgemeinen Regeln aus.
- Teilmenge der Richtlinieneinstellungen. Im Unterschied zur Richtlinie, in der alle Einstellungen enthalten sind, enthält ein Profil nur jene Einstellungen, die wirklich erforderlich sind (für die ein Schloss definiert ist).
- Die Aktivierungsbedingung ist ein logischer Ausdruck über den Eigenschaften des Geräts. Das Profil ist nur aktiv (ergänzt die Richtlinie), wenn die Aktivierungsbedingung des Profils erfüllt ist. In den übrigen Fällen ist das Profil inaktiv und wird ignoriert. Am logischen Ausdruck können die folgenden Geräteigenschaften teilnehmen:
  - Status des Modus für mobile Benutzer.
  - Die Eigenschaften der Netzwerkumgebung – der Name der aktiven Regel zur Verbindung des Administrationsagenten.
  - Vorhandensein oder Abwesenheit der angegebenen Tags auf dem Gerät.
  - Der Standort des Geräts im Active Directory-Einheit: explizit (das Gerät befindet sich unmittelbar in der angegebenen Organisationseinheit) oder implizit (das Gerät befindet sich in einer Organisationseinheit, die sich auf einer beliebigen Verschachtelungsebene innerhalb der angegebenen Organisationseinheit befindet).
  - Zugehörigkeit des Geräts zur Sicherheitsgruppe Active Directory (explizit oder implizit).
  - Zugehörigkeit des Gerätebesitzers zur Sicherheitsgruppe Active Directory (explizit oder implizit).

- Kontrollkästchen zum Deaktivierens des Profils. Deaktivierten Profile werden immer ignoriert, ihre Aktivierungsbedingungen werden nicht auf den Wahrheitsgehalt geprüft.

- Priorität des Profils. Die Aktivierungsbedingungen der Profile sind unabhängig, deshalb können mehrere Profile sofort gleichzeitig aktiviert werden. Wenn sich die aktiven Profile Einstellungssätze enthalten, die sich überschneiden, entstehen keine Probleme. Wenn jedoch zwei aktive Profile verschiedene Werte für ein und dieselbe Einstellung enthalten, entsteht eine Mehrdeutigkeit. Diese Mehrdeutigkeit wird mithilfe der Prioritäten der Profile entfernt: der Wert für die mehrdeutigen Variablen dem Profil mit der höheren Priorität (jenem Profil, das sich weiter oben in der Liste der Profile befindet) entnommen.

Verhalten der Profile bei der gegenseitigen Aktion der Richtlinien gemäß der Hierarchie

Gleichnamige Profile werden gemäß den Regeln zur Vereinigung von Richtlinien zusammengeführt. Profile der oberen Richtlinie haben gegenüber den Profilen der unteren Richtlinie Priorität. Wenn in "oberen" Richtlinie eine Änderung der Einstellungen verboten ist (die Schaltfläche Schloss wurde geklickt), werden in der "unteren" Richtlinie Aktivierungsbedingungen des Profils aus der "oberen" Richtlinie verwendet. Wenn in der "oberen" Richtlinie die Änderung der Einstellungen erlaubt ist, werden die Aktivierungsbedingungen des Profils aus der "unteren" Richtlinie verwendet.

Da das Richtlinienprofil in den Aktivierungsbedingungen die Eigenschaft **Gerät im autonomen Modus** enthalten kann, wird die Funktionalität der Richtlinien für mobile Benutzer vollständig durch die Profile ersetzt und nicht länger unterstützt.

Die Richtlinie für eigenständige Benutzer kann Profile enthalten, deren Aktivierung jedoch erst erfolgen kann, wenn das Gerät in den Modus für mobile Benutzer wechselt.

Vererbung von Richtlinieneinstellungen

Eine Richtlinie wird für eine Administrationsgruppe festgelegt. Richtlinieneinstellungen können *geerbt* werden, das heißt, sie können auf die Untergruppen (untergeordneten Gruppen) der Administrationsgruppe, für die sie erstellt wurden, übertragen werden. Im Weiteren wird eine Richtlinie für eine übergeordnete Gruppe auch als *übergeordnete Richtlinie* bezeichnet.

Sie können zwei Erboptionen aktivieren oder deaktivieren: **Einstellungen aus Richtlinie der höheren Ebene erben** und **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen**:

- Wenn Sie **Einstellungen aus übergeordneter Richtlinie erben** für eine untergeordnete Richtlinie aktivieren und einige Einstellungen in der übergeordneten Richtlinie mit einem Schloss sperren, können Sie diese Einstellungen nicht für die untergeordnete Gruppe bearbeiten. Sie können jedoch Einstellungen ändern, die nicht in der übergeordneten Richtlinie mit einem Schloss gesperrt sind.

- Wenn Sie **Einstellungen aus übergeordneter Richtlinie erben** für eine untergeordnete Richtlinie deaktivieren, können Sie alle Einstellungen in der untergeordneten Gruppe bearbeiten, selbst wenn einige Einstellungen in der übergeordneten Richtlinie mit einem Schloss gesperrt sind.

- Wenn Sie **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen** in der übergeordneten Gruppe aktivieren, wird dadurch **Einstellungen aus übergeordneter Richtlinie erben** für alle untergeordneten Richtlinien aktiviert. In diesem Fall kann diese Option nicht für untergeordnete Richtlinien deaktiviert werden. Alle Einstellungen, die in der übergeordneten Richtlinie gesperrt sind, werden zwangsweise an untergeordnete Gruppen vererbt und können in den untergeordneten Gruppen nicht bearbeitet werden.

- In der Gruppe **Verwaltete Geräte** beeinflusst die Option **Einstellungen aus übergeordneter Richtlinie erben** keine anderen Einstellungen, da die Gruppe **Verwaltete Geräte** keine Gruppen höherer Ebene besitzt und somit keine Richtlinien erbt.

Standardmäßig ist die Option **Einstellungen aus übergeordneter Richtlinie erben** für eine neue Richtlinie aktiviert.

Wenn eine Richtlinie über Profile verfügt, erben alle untergeordneten Richtlinien diese Profile.

Richtlinien verwalten

Die zentrale Konfiguration der Einstellungen für die Programme, die auf den Client-Geräten installiert sind, erfolgt über Richtlinien.

Die Richtlinien, die für die Programme in der Administrationsgruppe erstellt wurden, werden auf der Registerkarte **Richtlinien** im Arbeitsbereich angezeigt. Vor dem Namen jeder Richtlinie steht ein Symbol, das deren Status anzeigt.

Nach Löschen der Richtlinie oder Außerkraftsetzung setzt das Programm die Arbeit mit den Einstellungen fort, die in der Richtlinie angegeben sind. Sie können diese Einstellungen später manuell ändern.

Die Richtlinie wird auf eine der folgenden Arten übernommen: Werden auf dem Gerät Echtzeitschutz-Aufgaben ausgeführt, werden bei der Ausführung der Aufgaben neue Einstellungen verwendet. Regelmäßige Aufgaben (Untersuchung auf Befehl, Datenbanken-Update) werden mit den unveränderten Einstellungen ausgeführt. Der nächste Start regelmäßiger Aufgaben erfolgt mit den geänderten Einstellungen.

Richtlinien für Programme mit Unterstützung von Mandantenfähigkeit werden an Administrationsgruppen niedrigerer Stufen sowie an Administrationsgruppen höherer Stufen vererbt: die Richtlinie wird an alle Client-Geräte verteilt, auf denen das Programm installiert ist.

Bei einer hierarchischen Struktur der Administrationsserver empfangen die sekundären Administrationsserver Richtlinien vom primären Administrationsserver und verteilen sie auf die Client-Geräte. Ist die Vererbung aktiviert, lassen sich die Richtlinieneinstellungen auf dem primären Administrationsserver ändern. Nach dieser Änderung werden die Richtlinien, die auf die Einstellungen übernommen wurden, auf die vererbten Richtlinien auf den sekundären Administrationsservern übernommen.

Sollte die Verbindung zwischen dem primären Administrationsserver und sekundären Administrationsservern getrennt werden, gilt die Richtlinie auf dem sekundären Server mit den vorangegangenen Einstellungen weiter. Die auf dem primären Administrationsserver geänderten Richtlinieneinstellungen werden nach Wiederherstellung der Verbindung auf den sekundären Administrationsserver übertragen.

Ist die Vererbung deaktiviert, lassen sich die Richtlinieneinstellungen auf dem sekundären Administrationsserver ändern, und zwar unabhängig vom primären Administrationsserver.

Wird die Verbindung zwischen Administrationsserver und Client-Gerät getrennt, tritt auf dem Gerät die Richtlinie für mobile Benutzer in Kraft (wenn definiert) oder es gilt die Richtlinie mit den vorangegangenen Einstellungen weiter bis zur Wiederherstellung der Verbindung.

Die Ergebnisse für die Verteilung der Richtlinie auf die sekundären Administrationsserver werden im Eigenschaftenfenster der Richtlinie auf dem primären Administrationsserver angezeigt.

Die Ergebnisse der Verteilung der Richtlinie auf die Client-Geräte werden im Eigenschaftenfenster der Richtlinie des Administrationsservers angezeigt, mit dem die Client-Geräte verbunden sind.

Verwenden Sie in den Einstellungen der Richtlinien keine vertraulichen Daten. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Richtlinie erstellen

In der Verwaltungskonsole können Richtlinien unmittelbar im Ordner der Administrationsgruppe, für den die Richtlinie erstellt wird, und im Arbeitsbereich des Ordners **Richtlinien** erstellt werden.

Um eine Richtlinie im Ordner einer Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für welche die Richtlinie erstellt werden soll.
2. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien** aus.
3. Starten Sie mithilfe der Schaltfläche **Neue Richtlinie** den Assistenten für das Erstellen einer Richtlinie.

   Daraufhin wird der Assistent für das Erstellen einer Richtlinie gestartet. Folgen Sie den Anweisungen des Assistenten.

*Um eine Richtlinie im Arbeitsbereich des Ordners **Richtlinien** zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Starten Sie mithilfe der Schaltfläche **Neue Richtlinie** den Assistenten für das Erstellen einer Richtlinie.

   Daraufhin wird der Assistent für das Erstellen einer Richtlinie gestartet. Folgen Sie den Anweisungen des Assistenten.

In der Gruppe lassen sich für eine Anwendung mehrere Richtlinien erstellen, von denen aber immer nur eine Richtlinie aktiv sein kann. Beim Erstellen einer neuen, aktiven Richtlinie wird die vorangegangene aktive Richtlinie inaktiv.

Beim Erstellen einer Richtlinie können Sie Minimaleinstellungen anpassen, die für die Ausführung des Programms notwendig sind. Die übrigen Einstellungen behalten die Standardwerte und stimmen mit den Standardwerten bei der lokalen Anwendungsinstallation überein. Sie können die Richtlinie nach dem Erstellen ändern.

Verwenden Sie in den Einstellungen der Richtlinien keine vertraulichen Daten. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Einstellungen von Kaspersky-Anwendungen, die nach der Richtlinienübernahme geändert werden, werden in entsprechenden Handbüchern ausführlich beschrieben.

Nach dem Erstellen der Richtlinie treten die Einstellungen, deren Änderungen verboten sind (markiert mittels Schloss-Symbol ( )), auf den Client-Geräten in Kraft, unabhängig davon, welche Einstellungen für das Programm zuvor festgelegt wurden.

Vererbte Richtlinie in der untergeordneten Gruppe darstellen

Um die Anzeige einer vererbten Richtlinie für eine untergeordnete Administrationsgruppe zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für welche die vererbten Richtlinien angezeigt werden sollen.
2. Wählen Sie im Arbeitsbereich der gewählten Gruppe die Registerkarte **Richtlinien** aus.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinienliste und wählen **Ansicht** → **Geerbte Richtlinien**.

Daraufhin werden die geerbten Richtlinien mit dem Symbol in der Richtlinienliste angezeigt.

- – Wenn sie von der Gruppe vererbt wurden, die auf dem primären Administrationsserver erstellt wurde.
- – Wenn sie von der Gruppe der obersten Ebene vererbt wurden.

Wenn der Modus zum Vererben von Einstellungen aktiviert ist, können die vererbten Richtlinien nur in der Gruppe geändert werden, in der sie erstellt wurden. Die vererbten Richtlinien können nicht in der Gruppe geändert werden, welche die Richtlinien geerbt hat.

Richtlinien aktivieren

Um eine Richtlinie für die gewählte Gruppe zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsbereich der Gruppe auf der Registerkarte **Richtlinien** die Richtlinie aus, die aktiviert werden soll.
2. Zur Aktivierung der Richtlinie gehen Sie auf eine der folgenden Arten vor:
   - Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Aktive Richtlinie** aus.
   - Öffnen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Allgemein**, und wählen Sie in der Einstellungsgruppe **Richtlinienstatus** die Option **Aktive Richtlinie** aus.

Daraufhin wird die Richtlinie für die gewählte Administrationsgruppe aktiviert.

Wenn die Richtlinie eine Weile auf einer großen Anzahl von Client-Geräten angewendet wird, erhöhen sich die Belastung für den Administrationsserver und der Umfang des Datenverkehrs im Netzwerk erheblich.

Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren

Damit eine Richtlinie beim Eintritt eines Ereignisses "Virenangriff" automatisch aktiviert wird, gehen Sie wie folgt vor:

1. Öffnen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Virenangriff**.
2. Öffnen Sie das Fenster **Aktivierung von Richtlinien** durch Anklicken des Links **Richtlinien so konfigurieren, dass sie aktiviert werden, wenn ein Ereignis des Typs "Virenangriff" auftritt** und fügen Sie die Richtlinie der ausgewählten Liste von Richtlinien hinzu, die aktiviert werden, wenn ein Virenangriff erkannt wird.

Wird eine Richtlinie aufgrund des Ereignisses *Virenangriff* aktiviert, ist eine Rückkehr zur vorherigen Richtlinie nur manuell möglich.

Richtlinie für mobile Benutzer übernehmen

Die Richtlinie für mobile Benutzer tritt auf einem Gerät in Kraft, wenn das Gerät vom Firmennetzwerk getrennt wird.

Um eine Richtlinie für mobile Benutzer anzuwenden:

Wählen Sie in dem sich öffnenden Eigenschaftenfenster der Richtlinie den Abschnitt **Allgemein** und in den Gruppeneinstellungen **Richtlinienstatus** die Option **Richtlinie für mobile Benutzer** aus.

Die Richtlinie für mobile Benutzer tritt anschließend auf den Geräten in Kraft, wenn sie vom Firmennetzwerk getrennt werden.

Richtlinie ändern. Rollback der Änderungen

Um eine Richtlinie zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Richtlinien** die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
3. Nehmen Sie die notwendigen Änderungen vor.
4. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die Änderungen der Richtlinie werden in den Eigenschaften der Richtlinie, im Abschnitt **Revisionsverlauf** gespeichert.

Notfalls können Sie die Änderungen der Richtlinie zurücksetzen.

Um die Änderungen einer Richtlinie zurückzusetzen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Wählen Sie die Richtlinie, deren Änderungen zurückgesetzt werden sollen, aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
3. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Revisionsverlauf** aus.
4. Wählen Sie in der Liste mit den Richtlinienrevisionen die Nummer der Revision aus, deren Änderungen zurückgesetzt werden sollen.
5. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Rollback**.

Vergleich von Richtlinien

Sie können zwei Richtlinien für ein verwaltetes Programm vergleichen. Infolge des Vergleichs von Richtlinien erhalten Sie einen Bericht, in dem angezeigt wird, welche Einstellungen der Richtlinie übereinstimmen und welche sich unterscheiden. Ein Vergleich von Richtlinien ist notwendig, wenn beispielsweise verschiedene Administratoren in den lokalen Büros mehrere Richtlinien für ein verwaltetes Programm erstellt haben oder wenn einer Richtlinie der obersten Ebene vererbt und für jedes lokale Büro geändert wurde. Sie können die Richtlinien auf zwei Arten vergleichen: eine Richtlinie auswählen und mit einer anderen vergleichen oder zwei Richtlinien aus der Liste der Richtlinien vergleichen.

Sie können nur Richtlinien vergleichen, in deren Revisionsverläufen aktuelle Revisionen enthalten sind.

Um eine Richtlinie mit einer anderen zu vergleichen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Richtlinien** die Richtlinie aus, die mit einer anderen Richtlinie verglichen werden soll.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Richtlinie mit anderer Richtlinie vergleichen** aus.
4. Wählen Sie im Fenster **Richtlinie auswählen** die Richtlinie aus, mit der verglichen werden soll.
5. Klicken Sie auf die Schaltfläche **OK**.

Es wird ein Bericht über den Vergleich zweier Richtlinien für das Programm im html-Format angezeigt.

Um zwei Richtlinien aus der Liste der Richtlinien zu vergleichen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Richtlinien** in der Liste der Richtlinien mithilfe der Tasten **`Umschalt`** oder **`Strg`** zwei Richtlinien für ein verwaltetes Programm aus.
2. Wählen Sie im Kontextmenü den Punkt **Vergleichen** aus.

Es wird ein Bericht über den Vergleich zweier Richtlinien für das Programm im html-Format angezeigt.

Im Bericht über den Vergleich der Richtlinieneinstellungen für das Programm Kaspersky Endpoint Security für Windows wird auch der Vergleich der Richtlinienprofile ausgeführt. Die Ergebnisse des Vergleiches der Einstellungen der Richtlinienprofile können minimiert werden. Um einen Block zu minimieren, klicken Sie auf das Pfeil-Symbol ( ) neben dem Namen des Blocks.

Diagramm zum Status der Richtlinienverteilung anzeigen

In Kaspersky Security Center können Sie die Ergebnisse der Richtliniendurchsetzung auf jedem Gerät anzeigen.

So zeigen Sie das Statusdiagramm für die Richtlinienverteilung für jedes Gerät an:

1. Wählen Sie im Arbeitsbereich der Gruppe auf der Registerkarte **Richtlinien** die Richtlinie aus, deren Verteilungsstatus Sie anzeigen möchten.

   Das Diagramm im rechten Abschnitt zeigt eine Übersicht über die Richtliniendurchsetzung an.

2. Kicken Sie auf **Details**.

   Das Fenster **Ergebnisse der Richtlinienanwendung** wird geöffnet.

   Sie können die Ergebnisse der Richtliniendurchsetzung als csv- oder txt-Datei exportieren.

Richtlinien löschen

Um eine Richtlinie zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsbereich der Administrationsgruppe auf der Registerkarte **Richtlinien** die Richtlinie aus, die gelöscht werden soll.

2. Löschen Sie die Richtlinie auf eine der folgenden Arten:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Löschen** aus.

   - Klicken Sie auf den Link **Richtlinie löschen** im Informationsfeld der ausgewählten Richtlinie.

Richtlinien kopieren

Um eine Richtlinie zu kopieren, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsbereich der gewünschten Gruppe auf der Registerkarte **Richtlinien** die entsprechende Richtlinie aus.

2. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Kopieren** aus.

3. Wählen Sie in der Konsolenstruktur die Gruppe aus, zu der die Richtlinie hinzugefügt werden soll.

   Die Richtlinie kann zur selben Gruppe hinzugefügt werden, aus der sie kopiert wurde.

4. Klicken Sie mit der rechten Maustaste auf die Richtlinienliste für die gewählte Gruppe auf der Registerkarte **Richtlinien** und wählen Sie **Einfügen** aus.

Daraufhin wird die Richtlinie mit allen Einstellungen kopiert und auf alle Geräte der Gruppe verteilt, auf die sie übertragen wurde. Wenn Sie die Richtlinie in dieselbe Gruppe einfügen, von der sie kopiert wurde, wird dem Namen der Richtlinie automatisch die Endung der Form **(<laufende Nummer>)** hinzugefügt. Beispiel: **(1)**, **(2)**.

Eine aktive Richtlinie wird nach dem Kopieren inaktiv. Sie können bei Bedarf die Richtlinie aktivieren.

Richtlinien exportieren

Um eine Richtlinie zu exportieren, gehen Sie wie folgt vor:

1. Exportieren Sie die Richtlinie auf eine der folgenden Arten:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Alle Aufgaben** → **Exportieren** aus.
   - Klicken Sie auf den Link **Richtlinie in Datei exportieren** im Informationsfeld der ausgewählten Richtlinie.

2. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Richtliniendatei zum Speichern an. Klicken Sie auf **Speichern**.

Richtlinien importieren

So importieren Sie eine Richtlinie:

1. Wählen Sie im Arbeitsbereich der betreffenden Gruppe auf der Registerkarte **Richtlinien** eine der folgenden Methoden für den Import der Richtlinie aus:

   - Wählen Sie im Kontextmenü der Richtlinienliste den Punkt **Alle Aufgaben** → **Importieren** aus.
   - Klicken Sie im Block zur Verwaltung der Richtlinienliste auf **Richtlinie aus Datei importieren**.

2. Geben Sie im folgenden Fenster den Pfad zu der Datei an, aus der Sie die Richtlinie importieren wollen. Klicken Sie auf **Öffnen**.

Die importierte Richtlinie wird in der Liste mit den Richtlinien angezeigt. Die Einstellungen und Profile der Richtlinie werden ebenfalls importiert. Unabhängig vom Richtlinienstatus, der während des Exports ausgewählt wurde, ist die importierte Richtlinie inaktiv. Sie können den Richtlinienstatus in den Eigenschaften der Richtlinie ändern.

Wenn die neu importierte Richtlinie denselben Namen wie eine bereits vorhandene Richtlinie besitzt, wird der Name der importierten Richtlinie um den Index **(<nächste Sequenznummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Richtlinien konvertieren

Kaspersky Security Center ermöglicht es, die Richtlinien vorheriger Versionen der von verwalteten Kaspersky-Anwendungen in die Richtlinien aktueller Versionen derselben Programme zu konvertieren. Konvertierte Richtlinien behalten die aktuellen Administratoreinstellungen bei, die vor der Aktualisierung festgelegt wurden, und enthalten neue Einstellungen aus den aktuellen Versionen der Programme. Wenn eine Richtlinie in die aktuelle Version eines verwalteten Programms von Kaspersky konvertiert wird, können Sie die Richtlinie nicht auf einem Administrationsserver öffnen, auf dem eine frühere Version des Programm-Plug-ins installiert ist. Verwaltungs-Plug-ins für Kaspersky-Anwendungen bestimmen, ob die Konvertierung für die Richtlinien dieser Programme verfügbar ist. Weitere Informationen zum Konvertieren von Richtlinien können Sie für jede unterstützte Kaspersky-Anwendung aus der entsprechenden Hilfe in folgender Liste entnehmen:

- **Kaspersky-Anwendungen für Workstations:**
  - Kaspersky Endpoint Security für Windows
  - Kaspersky Endpoint Security für Linux
  - Kaspersky Endpoint Security für Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security für Windows
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (zentralisierte Bereitstellung wird nicht unterstützt)
- **Kaspersky-Anwendungen für mobile Geräte:**
  - Kaspersky Endpoint Security für Android
  - Kaspersky Security für iOS
- **Kaspersky-Anwendungen für Dateiserver:**
  - Kaspersky Security für Windows Server
  - Kaspersky Endpoint Security für Windows
  - Kaspersky Endpoint Security für Linux
- **Kaspersky-Anwendungen für virtuelle Maschinen:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless

- **Kaspersky-Anwendungen zur Erkennung gezielter Angriffe:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **Kaspersky-Anwendungen für KasperskyOS-Geräte:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (Plug-in für Kaspersky Thin Client)

Um Richtlinien konvertieren zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus, für den Richtlinien konvertiert werden sollen.
2. Wählen Sie im Kontextmenü des Administrationsservers den Punkt **Alle Aufgaben → Assistent für das Massenkonvertieren von Richtlinien und Aufgaben**.

   Daraufhin wird der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben gestartet. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten werden neue Richtlinien erstellt, welche die Richtlinieneinstellungen des aktuellen Administrators und die neuen Einstellungen aus den aktuellen Versionen der Kaspersky-Anwendungen verwenden.

Richtlinienprofile verwalten

Ein Richtlinienprofil ist eine benannte Auswahl von Richtlinieneinstellungen, die bei der Erfüllung von bestimmten Bedingungen auf dem Client-Gerät (Computer, mobiles Gerät) aktiviert wird, sofern das Gerät die festgelegten Aktivierungsregeln erfüllt. Bei der Aktivierung des Profils werden die Einstellungen der bis zur Aktivierung des Profils auf dem Gerät geltenden Richtlinie geändert. Diese Einstellungen nehmen die im Profil festgelegten Werte an.

Richtlinienprofile sind erforderlich, damit Geräte innerhalb einer Administrationsgruppe verschiedene Richtlinieneinstellungen haben konnten. Es ist beispielsweise eine Situation möglich, in der die Richtlinieneinstellungen in der Administrationsgruppe für einige Geräte geändert werden müssen. In diesem Fall können für eine solche Richtlinie Richtlinienprofile konfiguriert werden, bei deren Nutzung es möglich ist, die Richtlinieneinstellungen nicht für alle Geräte der Administrationsgruppe zu ändern. Beispielsweise verbietet eine Richtlinie den Start von jeglichen GPS-Navigationsprogrammen für alle Geräte der Administrationsgruppe "Benutzer". GPS-Navigationsprogramme sind nur für das Gerät eines Benutzers erforderlich, der in der Administrationsgruppe "Benutzer" die Rolle eines Kuriers ausführt. Diesem Gerät kann das Tag "Kurier" zugewiesen werden und anschließend kann das Richtlinienprofil so angepasst werden, dass es den Start der GPS-Navigationsprogramme nur auf dem Gerät mit dem Tag "Kurier" erlaubt, wobei alle übrigen Einstellungen der Richtlinie gespeichert werden. Taucht in diesem Fall in der Administrationsgruppe "Benutzer" ein Gerät mit dem Tag "Kurier" auf, wird auf diesem Gerät der Start der GPS-Navigationsprogramme erlaubt. Auf den anderen Geräten in der Administrationsgruppe "Benutzer", bei denen der Tag "Kurier" fehlt, ist der Start der GPS-Navigationsprogramme untersagt.

Die Profile werden nur für die folgenden Richtlinien unterstützt:

- Richtlinien von Kaspersky Endpoint Security für Windows.
- Richtlinien von Kaspersky Endpoint Security for Mac.
- Richtlinien des Plug-ins für Kaspersky Mobile Device Management der Versionen 10 Service Pack 1 bis 10 Service Pack 3 Maintenance Release 1.
- Richtlinien des Plug-ins für Kaspersky Device Management für iOS.
- Richtlinien des Programms Kaspersky Security for Virtualization 5.1 Light Agent for Windows.
- Richtlinien des Programms Kaspersky Security for Virtualization 5.1 Light Agent for Linux.

Richtlinienprofile erleichtern die Verwaltung von Client-Geräten, auf denen Richtlinien angewendet werden:

- Die Einstellungen des Richtlinienprofils können sich von den Einstellungen der Richtlinie selbst unterscheiden.
- Es ist nicht erforderlich, manuell mehrere Kopien einer Richtlinie zu unterstützen und anzuwenden, wenn sich diese nur durch wenige Einstellungen unterscheiden.
- Es ist keine separate Richtlinie für eigenständige Benutzer erforderlich.
- Sie können Richtlinienprofile exportieren und importieren, sowie neue Profile auf Basis der bestehenden erstellen.
- Für eine Richtlinie können mehrere Richtlinienprofile aktiv sein. Auf ein Gerät werden jene Profile angewendet, die den Aktivierungsregeln auf diesem Gerät entsprechen.
- Die Profile unterliegen der Hierarchie der Richtlinien. Eine untergeordnete Richtlinie enthält alle Richtlinienprofile der obersten Ebene.

Profilpriorität

Die für die Richtlinie erstellten Profile sind in absteigender Priorität gereiht. Wenn sich das Profil X beispielsweise in der Richtlinienliste über dem Profil Y befindet, hat das Profil X eine höhere Priorität als Y. Einem Gerät können mehrere Profile gleichzeitig zugewiesen werden. Wenn sich der Wert einer bestimmten Einstellung in den Profilen unterscheidet, wird auf dem Gerät der Einstellungswert aus jenem Profil verwendet, das die höhere Priorität hat.

Regeln für die Profilaktivierung

Richtlinienprofile werden auf dem Client-Gerät mithilfe von Aktivierungsregeln aktiviert. *Aktivierungsregeln* – Satz von Bedingungen, bei deren Ausführung das Richtlinienprofil auf dem Gerät ausgeführt wird. Aktivierungsregeln können folgende Bedingungen enthalten:

- Der Administrationsagent auf dem Client-Gerät stellt unter Berücksichtigung bestimmter Verbindungseinstellungen, beispielsweise der Adresse des Administrationsservers, Portnummer usw., eine Verbindung zum Server her.
- Das Client-Gerät befindet sich im autonomen Modus.
- Dem Client-Gerät sind bestimmte Tags zugewiesen.

- Das Client-Gerät befindet sich explizit (das Gerät befindet sich unmittelbar im angegebenen Unterverzeichnis) oder implizit (das Gerät befindet sich in einem Unterverzeichnis, das sich auf einer beliebigen Verschachtelungsebene innerhalb des angegebenen Unterverzeichnisses befindet) in einem bestimmten Unterverzeichnis des Active Directory®, das Gerät oder sein Besitzer befinden sich in der Sicherheitsgruppe von Active Directory.

- Das Client-Gerät gehört einem bestimmten Eigentümer oder der Eigentümer des Geräts befindet sich in einer internen Sicherheitsgruppe von Kaspersky Security Center.

- Dem Inhaber des Client-Geräts wurde eine festgelegte Rolle zugewiesen.

Richtlinien in hierarchischen Administrationsgruppen

Wenn Sie die Richtlinie in der Administrationsgruppe der unteren Ebene erstellen, so erbt die neue Richtlinie die Profile der aktiven Richtlinie für die Gruppe der obersten Ebene. Profile mit identischen Namen werden zusammengelegt. Die Richtlinienprofile für die Gruppe der höheren Ebene haben höhere Priorität. Beispielsweise umfasst die Richtlinie *P(A)* in der Administrationsgruppe *A* die Profile *X1*, *X2* und *X3* in absteigender Reihenfolge. In der Administrationsgruppe *B*, die eine Untergruppe von Gruppe *A* ist, wird die Richtlinie *P(B)* mit den Profilen *X2*, *X4* und *X5* erstellt. Somit wird die Richtlinie *P(B)* durch die Richtlinie *P(A)* geändert, weil die Liste der Profile in der Richtlinie *P(B)* in absteigender Reihenfolge *X1*, *X2*, *X3*, *X4*, *X5* lautet. Die Priorität von Profile *X2* hängt vom ursprünglichen Status von *X2* in der Richtlinie *P(B)* und *X2* in der Richtlinie *P(A)* ab. Nach dem Erstellen der Richtlinie *P(B)* wird die Richtlinie *P(A)* in der Untergruppe *B* nicht angezeigt.

Die aktive Richtlinie wird bei jedem Start des Administrationsagenten, bei der Aktivierung bzw. Deaktivierung des autonomen Modus sowie bei einer Änderung der dem Client-Gerät zugewiesenen Tag-Liste neu berechnet. Wenn beispielsweise auf einem Gerät der Umfang des Arbeitsspeichers vergrößert wurde, wird daraufhin das Richtlinienprofil aktiviert, das für Geräte mit größerem Arbeitsspeichers verwendet wird.

Eigenschaften und Beschränkungen von Richtlinienprofilen

Profile haben folgende Eigenschaften:

- Profile von nicht aktiven Richtlinien haben keine Auswirkung auf Client-Geräte.

- Wenn eine Richtlinie in den Status **Richtlinie für mobile Benutzer** versetzt wird, werden die Profile dieser Richtlinie auch dann angewandt, wenn das Gerät vom Unternehmensnetzwerk getrennt ist.

- Die statistische Zugriffsanalyse auf ausführbare Dateien wird von Profilen nicht unterstützt.

- Das Richtlinienprofil kann keine Einstellungen für Benachrichtigungen über Ereignisse enthalten.

- Wenn für die Verbindung des Geräts mit dem Administrationsserver der UDP-Port 15000 verwendet wird, aktiviert sich das entsprechende Richtlinienprofil bei der Zuweisung eines Tags auf dem Gerät innerhalb einer Minute.

- Sie können die Verbindungsregeln des Administrationsagenten zum Administrationsserver verwenden, wenn Sie die Aktivierungsregeln des Richtlinienprofils erstellen.

Richtlinienprofil erstellen

Profile können nur für die Richtlinien der folgenden Anwendungen erstellt werden:

- Kaspersky Endpoint Security 10 Service Pack 1 für Windows und höhere Versionen
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Plug-in für Kaspersky Mobile Device Management der Versionen 10 Service Pack 1 bis 10 Service Pack 3 Maintenance Release 1
- Kaspersky Device Management für iOS Plug-in
- Kaspersky Security for Virtualization 5.1 Light Agent für Windows und Linux

Um ein Richtlinienprofil zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für deren Richtlinie das Richtlinienprofil erstellt werden soll.
2. Wählen Sie im Arbeitsbereich der Administrationsgruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Richtlinienprofile** und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent zur Erstellung von Richtlinienprofilen wird gestartet.
5. Geben Sie im Fenster **Name des Richtlinienprofils** des Assistenten Folgendes an:

   a. Name des Richtlinienprofils

      Der Name des Profils darf nicht mehr als 100 Zeichen umfassen.

   b. Status des Richtlinienprofils (*Aktiviert*, *Deaktiviert*)

      Es wird empfohlen, inaktive Richtlinienprofile zu erstellen und sie erst nach dem vollständigen Abschluss der Konfiguration der Einstellungen und der Bedingungen zur Aktivierung der Richtlinienprofile zu aktivieren.
6. Aktivieren Sie das Kontrollkästchen **Nach Beendigung des Assistenten für das Erstellen eines Richtlinienprofils zur Konfiguration der Aktivierungsregeln für das Richtlinienprofil wechseln**, um den Assistenten für das Erstellen einer Aktivierungsregel eines Richtlinienprofils zu starten. Folgen Sie den Schritten des Assistenten.
7. Einstellungen der Richtlinienprofile im Fenster Einstellungen für Richtlinienprofile auf die erforderliche Art ändern.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

   Das Profil wird gespeichert. Das Profil wird auf Geräten aktiviert, auf denen die Aktivierungsregeln erfüllt sind.

Für eine Richtlinie können mehrere Richtlinienprofile erstellt werden. Profile, die für eine Richtlinie erstellt wurden, werden in den Eigenschaften der Richtlinie im Abschnitt **Richtlinienprofile** angezeigt. Sie können ein Richtlinienprofil ändern und die Priorität des Profils ändern sowie das Profil entfernen.

Richtlinienprofil ändern

Einstellungen eines Richtlinienprofils ändern

Richtlinienprofile können nur für Richtlinien von Kaspersky Endpoint Security für Windows geändert werden.

Um die Einstellungen eines Richtlinienprofils zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die das Richtlinienprofil geändert werden soll.
2. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
4. Öffnen Sie in den Eigenschaften der Richtlinie den Abschnitt **Richtlinienprofile**.

   Dieser Abschnitt enthält eine Liste der für diese Richtlinie erstellten Profile. Die Profile werden in der Liste entsprechend ihrer Priorität angezeigt.
5. Wählen Sie ein Richtlinienprofil und klicken Sie auf die Schaltfläche **Eigenschaften**.
6. Passen Sie im Eigenschaftenfenster die Einstellungen des Profils an:
   - Ändern Sie im Abschnitt **Allgemein** erforderlichenfalls den Namen des Profils und aktivieren bzw. deaktivieren Sie das Profil mithilfe des Kontrollkästchens **Profil aktivieren**.
   - Ändern Sie im Abschnitt **Aktivierungsregeln** die Aktivierungsregeln für das Profil.
   - Ändern Sie die Einstellungen der Richtlinie in den entsprechenden Abschnitten.
7. Klicken Sie auf die Schaltfläche **OK**.

Die geänderten Einstellungen werden nach der Synchronisierung des Geräts mit dem Administrationsserver (wenn das Richtlinienprofil aktiv ist) bzw. nach der Ausführung der Aktivierungsregeln (wenn das Richtlinienprofil nicht aktiv ist) angewendet.

Priorität eines Richtlinienprofils ändern

Durch die Priorität von Richtlinienprofilen wird die Aktivierungsreihenfolge der Profile auf dem Client-Gerät bestimmt. Die Priorität wird verwendet, wenn für verschiedene Richtlinienprofile die gleichen Aktivierungsregeln festgelegt sind.

Beispielsweise wurden die beiden Richtlinienprofile *Profil 1* und *Profil 2* erstellt, die sich voneinander durch den Wert einer Einstellung unterscheiden (*Wert 1* und *Wert 2*). Die Priorität von *Profil 1* ist höher als die Priorität von *Profil 2*. Außerdem existieren Profile mit einer niedrigeren Priorität als *Profil 2*. Die Aktivierungsregeln der Profile stimmen überein.

Bei der Ausführung der Aktivierungsregeln wird *Profil 1* aktiviert. Die Einstellung auf dem Gerät nimmt den *Wert 1* an. Wenn *Profil 1* gelöscht wird, erhält *Profil 2* die höchste Priorität und die Einstellung nimmt den *Wert 2* an.

In der Liste der Richtlinienprofile werden die Profile entsprechend ihrer Priorität angezeigt. An erster Stelle der Liste steht das Profil mit der höchsten Priorität. Die Priorität der Profile kann mithilfe der Nach-oben-Schaltfläche  und der Nach-unten-Schaltfläche  geändert werden.

Richtlinienprofil löschen

Um ein Richtlinienprofil zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die das Richtlinienprofil gelöscht werden soll.
2. Wählen Sie im Arbeitsbereich der Administrationsgruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
4. Öffnen Sie in den Eigenschaften der Richtlinie für Kaspersky Endpoint Security den Abschnitt **Richtlinienprofile**.
5. Wählen Sie das zu löschende Richtlinienprofil aus und klicken Sie auf **Löschen**.

Das Richtlinienprofil wird gelöscht. Aktiv wird entweder ein anderes Richtlinienprofil, dessen Aktivierungsregeln auf dem Gerät ausgeführt werden, oder eine Richtlinie.

Regeln für die Aktivierung des Richtlinienprofils erstellen

Um eine Regel für die Aktivierung des Richtlinienprofils zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die eine Regel für die Aktivierung des Richtlinienprofils erstellt werden soll.
2. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Richtlinienprofile** aus.
5. Wählen Sie das Richtlinienprofil aus, für das eine Aktivierungsregel erstellt werden soll, und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Daraufhin wird das Eigenschaftenfenster des Richtlinienprofils geöffnet.

   Wenn die Richtlinienprofilliste leer ist, können Sie ein Richtlinienprofil erstellen.
6. Wählen Sie den Bereich **Aktivierungsregeln** und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird der Assistent für das Erstellen einer Aktivierungsregel eines Richtlinienprofils gestartet.

7. Aktivieren Sie im Fenster **Regeln für die Aktivierung des Richtlinienprofils** die Kontrollkästchen neben den Bedingungen, die Einfluss auf die Aktivierung des erstellten Richtlinienprofils haben sollen:

   - **Allgemeine Regeln für die Aktivierung des Richtlinienprofils**

     Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät je nach dem Zustand des autonomen Modus des Geräts, der Verbindungsregel des Geräts mit dem Administrationsserver und den dem Gerät zugewiesenen Tags anzupassen.

   - **Regeln für die Verwendung von Active Directory**

     Aktivieren Sie dieses Kontrollkästchen, um die Aktivierungsregeln für das Richtlinienprofil auf dem Gerät anzupassen. Die Regeln sind davon abhängig, ob das Gerät in einer Active Directory-Organisationseinheit (OU) vorhanden ist oder ob das Gerät (oder dessen Eigentümer) zu einer Active Directory-Sicherheitsgruppe gehört.

   - **Regeln für einen bestimmten Gerätebesitzer**

     Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät abhängig vom Gerätebesitzer und von der Zugehörigkeit des Geräts zur internen Sicherheitsgruppen von Kaspersky Security Center anzupassen.

   - **Regeln für Hardware-Eigenschaften**

     Aktivieren Sie das Kontrollkästchen, um auf dem Gerät die Aktivierung der Richtlinienprofile je nach Speichergröße und Anzahl seiner logischen Prozesse anzupassen.

   Von der Auswahl der Einstellungen im ersten Schritt hängt die weitere Anzahl der Seiten des Assistenten ab. Sie können die Regeln für die Richtlinienprofilaktivierung später ändern.

8. Geben Sie in dem Fenster **Allgemeine Bedingungen** die folgenden Einstellungen an:

   - Geben Sie im Feld **Gerät im autonomen Modus** in der Dropdown-Liste die Bedingung für den Speicherort des Geräts im Netzwerk an:

     - **Ja**

       Das Gerät befindet sich in einem externen Netzwerk, daher ist der Administrationsserver nicht verfügbar.

     - **Nein**

       Das Gerät befindet sich im Netzwerk, somit ist der Administrationsserver verfügbar.

     - **Es wurde kein Wert gewählt**

       Es wird kein Kriterium angewandt.

   - Passen Sie im Feld **Das Gerät befindet sich im angegebenen Netzwerkstandort** mithilfe der Dropdown-Listen die Aktivierung des Richtlinienprofils beim Erfüllen/Nichterfüllen der Regeln für die Verbindung mit dem Administrationsserver auf dem Gerät an:

     - **Erfüllt / Erfüllt nicht**

       Aktivierungsbedingung für das Richtlinienprofil (Regel wird erfüllt bzw. nicht erfüllt)

     - **Regelname**

       Beschreibung des Netzwerkspeicherorts des Geräts für die Verbindung mit dem Administrationsserver für die Aktivierung des Richtlinienprofils beim Erfüllen bzw. Nichterfüllen von dessen Bedingungen.

Die Beschreibung des Netzwerkspeicherorts der Geräte für die Verbindung mit dem Administrationsserver kann erstellt oder in der Regel für die Umschaltung des Administrationsagenten angepasst werden.

Das Fenster **Allgemeine Bedingungen** wird angezeigt, wenn das Kontrollkästchen **Allgemeine Regeln für die Aktivierung des Richtlinienprofils** aktiviert wurde.

9. Geben Sie in dem Fenster **Bedingungen unter Verwendung von Tags** die folgenden Einstellungen an:

   - **Liste der Tags**

     Geben Sie in der Liste der Tags Aktivierungsregeln für Geräte im Richtlinienprofil an, indem Sie die Kontrollkästchen der entsprechenden Tags aktivieren.

     Sie können neue Tags zur Liste hinzufügen, indem Sie diese im Feld über der Liste eingeben und auf die Schaltfläche **Hinzufügen** klicken.

     Das Richtlinienprofil erstreckt sich auf Geräte, in deren Beschreibung alle ausgewählten Tags vorkommen. Sind Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt. Standardmäßig sind die Kontrollkästchen deaktiviert.

   - **Auf Geräte ohne angegebene Tags anwenden**

     Aktivieren Sie die Option, wenn die Auswahl der Tags invertiert werden muss.

     Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in das Richtlinienprofil aufgenommen. Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

     Diese Option ist standardmäßig deaktiviert.

   Das Fenster **Bedingungen unter Verwendung von Tags** wird angezeigt, wenn das Kontrollkästchen **Allgemeine Regeln für die Aktivierung des Richtlinienprofils** aktiviert ist.

10. Geben Sie in dem Fenster **Bedingungen bei Verwendung von Active Directory** die folgenden Einstellungen an:

    - **Zugehörigkeit des Gerätebesitzers zur Sicherheitsgruppe Active Directory**

      Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert, wenn dessen Inhaber Mitglied der angegebenen Sicherheitsgruppe ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

    - **Zugehörigkeit des Geräts zur Sicherheitsgruppe Active Directory**

      Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

    - **Gerätezuordnung in der Active Directory-Organisationseinheit**

      Bei aktivierter Option wird das Richtlinienprofil auf einem Gerät aktiviert, das explizit oder implizit in der angegebenen Active Directory-Organisationseinheit (OU) enthalten ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt.

      Diese Option ist standardmäßig deaktiviert.

    Das Fenster **Bedingungen bei Verwendung von Active Directory** wird angezeigt, wenn das Kontrollkästchen **Regeln für die Verwendung von Active Directory** aktiviert ist.

11. Geben Sie in dem Fenster **Bedingungen bei Verwendung des Gerätebesitzers** die folgenden Einstellungen an:

    - **Gerätebesitzer**

      Aktivieren Sie die Option, um die Aktivierungsregel des Profils auf dem Gerät anhand des Geräteinhabers anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

      - Gerät gehört dem angegebenen Inhaber ("="-Symbol).
      - Gerät gehört nicht dem angegebenen Inhaber ("#"-Symbol).

        Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können den Gerätebesitzer angeben, wenn die Option aktiviert ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

    - **Der Gerätebesitzer gehört zur internen Sicherheitsgruppe**

      Aktivieren Sie die Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Zugehörigkeit des Geräteinhabers zur internen Sicherheitsgruppe von Kaspersky Security Center anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

      - Der Gerätebesitzer gehört zur angegebenen Sicherheitsgruppe ("="-Symbol).
      - Der Gerätebesitzer gehört nicht zur angegebenen Sicherheitsgruppe ("#"-Symbol).

        Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können eine Sicherheitsgruppe von Kaspersky Security Center angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

    - **Richtlinienprofil durch eine bestimmte Rolle des Gerätebesitzers aktivieren**

      Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät in Abhängigkeit von der Rolle des Besitzers zu konfigurieren. Fügen Sie die Rolle manuell aus der Liste vorhandener Rollen hinzu.

      Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt.

    Das Fenster **Bedingungen bei Verwendung des Gerätebesitzers** wird angezeigt, wenn das Kontrollkästchen **Regeln für einen bestimmten Gerätebesitzer** aktiviert ist.

12. Geben Sie in dem Fenster **Bedingungen bei Verwendung von Hardwareeigenschaften** die folgenden Einstellungen an:

    - **Speichergröße (MB)**

      Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Arbeitsspeichergröße des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

      - Arbeitsspeicher des Geräts kleiner als festgelegter Wert (Zeichen "<")
      - Arbeitsspeicher des Geräts größer als festgelegter Wert (Zeichen ">")

Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Größe des Arbeitsspeichers auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Anzahl der logischen Prozesse**

  Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Anzahl der logischen Prozessoren des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

  - Anzahl der logischen Prozesse des Geräts kleiner oder gleich festgelegter Wert (Zeichen "<")
  - Anzahl der logischen Prozesse des Geräts größer oder gleich festgelegter Wert (Zeichen ">")

  Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Anzahl der logischen Prozessoren auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

Das Fenster **Bedingungen bei Verwendung von Hardwareeigenschaften** wird angezeigt, wenn das Kontrollkästchen **Regeln für Hardware-Eigenschaften** aktiviert ist.

13. Im Fenster **Name der Regel für die Aktivierung des Richtlinienprofils**, im Feld **Regelname** geben Sie einen Namen für die Regel ein.

Das Profil wird gespeichert. Das Profil wird auf dem Gerät aktiviert, wenn die Aktivierungsregel ausgeführt wird.

Die Regeln für die Aktivierung des Richtlinienprofils, die für das Profil erstellt wurden, werden in den Eigenschaften des Richtlinienprofils in dem Abschnitt **Aktivierungsregeln** angezeigt. Sie können die Regel für die Aktivierung des Richtlinienprofils ändern oder löschen.

Mehrere Aktivierungsregeln können gleichzeitig ausgeführt werden.

Verschiebungsregeln für Geräte

Es wird empfohlen, die Verteilung von Geräten auf Administrationsgruppen mithilfe der *Regeln für das Verschieben von Geräten* zu automatisieren. Die Regel zum Verschieben besteht aus drei Hauptteilen: dem Namen, der Ausführungsbedingung (ein logischer Ausdruck über die Attribute des Geräts) und der Zieladministrationsgruppe. Die Regel verschiebt das Gerät in die Zieladministrationsgruppe, wenn die Attribute des Geräts die Bedingung für die Regelausführung erfüllen.

Alle Regeln für das Verschieben von Geräten haben Prioritäten. Der Administrationsserver prüft die Attribute des Geräts auf Übereinstimmung mit der Bedingung für die jeweilige Regelausführung in abnehmender Priorität der Regeln. Wenn die Attribute des Geräts die Bedingungen für die Regelausführung erfüllen, wird das Gerät in die Zielgruppe verschoben und beendet daraufhin die Verarbeitung der Regeln für das betreffende Gerät. Wenn die Attribute des Geräts sofort einigen Regeln entsprechen, wird das Gerät in die Zielgruppe jener Regel verschoben, welche die höchste Priorität hat (in der Liste der Regeln weiter oben steht).

Die zum Geräte verschieben können implizit erstellt werden. Beispielsweise kann in den Eigenschaften des Installationspakets oder der Aufgabe zur Remote-Installation die Administrationsgruppe angegeben werden, in die das Gerät gelangen soll, nachdem darauf der Administrationsagent installiert wurde. Darüber hinaus können die Regeln zum Verschieben vom Administrator von Kaspersky Security Center auf offensichtliche Art in der Liste der Regeln zum Verschieben erstellt werden. Die Liste befindet sich in der Verwaltungskonsole in den Eigenschaften der Gruppe **Nicht zugeordnete Geräte**.

Die Regel zum Verschiebung ist standardmäßig für eine einmalige erstmalige Verteilung der Geräte auf die Administrationsgruppen vorgesehen. Die Regel verschiebt die Geräte, die sich in der Gruppe **Nicht zugeordnete Geräte** befinden, nur einmal. Wenn ein Gerät von dieser Regel einmal verschoben wurde, wird es nicht nochmals von der Regel verschoben, selbst wenn das Gerät manuell erneut in die Gruppe **Nicht zugeordnete Geräte** verschoben wird. Dies ist die empfohlene Art der Nutzung der Regeln zum Verschieben.

Es können Geräte verschoben werden, die sich bereits in Administrationsgruppen befinden. Dazu muss in den Eigenschaften der Regel das Kontrollkästchen **Nur Geräte verschieben, die keiner Administrationsgruppe angehören** deaktiviert werden.

Durch die Existenz von Regeln zum Verschieben, die auf Geräte gelten, die bereits in die Administrationsgruppen verschoben wurden, steigt die Belastung auf dem Administrationsserver erheblich.

In den Eigenschaften von automatisch erstellten Verschiebungsregeln ist das Kontrollkästchen **Nur Geräte verschieben, die keiner Administrationsgruppe angehören** gesperrt. Diese Regeln werden erstellt, wenn Sie die Aufgabe *Remote-Installation einer Anwendung* hinzufügen oder ein autonomes Installationspaket erstellen.

Es kann eine Regel zum Verschieben erstellt werden, die auf einem Gerät mehrfach ausgeführt werden kann.

Es wird dringend empfohlen, Szenarien zu vermeiden, bei denen ein verwaltetes Gerät mehrfach aus einer Gruppe in eine andere verschoben wird (z. B. um eine besondere Richtlinie auf das Gerät anzuwenden, eine spezielle Gruppenaufgabe zu starten oder das Gerät über einen bestimmten Verteilungspunkt zu aktualisieren).

Solche Szenarien werden nicht unterstützt, da sie die Belastung des Administrationsservers und den Datenverkehr in extremem Ausmaß erhöhen. Diese Szenarien stehen ferner in Konflikt mit den Betriebsprinzipien von Kaspersky Security Center (insbesondere im Bereich von Zugriffsrechen, Ereignissen und Berichten). Es müssen andere Lösungen gesucht werden, zum Beispiel durch Verwendung der Richtlinienprofile, der Aufgaben für Geräteauswahlen und der Zuweisung von Administrationsagenten entsprechend dem Standardszenario.

Klonen von Regeln für das Verschieben von Geräten

Wenn Sie über mehrere Regeln für das Verschieben von Geräten mit ähnlichen Einstellungen verfügen, können Sie eine bestehende Regel klonen und anschließend die Einstellungen der geklonten Regel ändern. Das ist beispielsweise dann sinnvoll, wenn Sie mehrere identische Regeln für das Verschieben von Geräten mit unterschiedlichen IP-Bereichen und Zielgruppen benötigen.

Um eine Regel für das Verschieben von Geräten zu klonen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im Ordner **Nicht zugeordnete Geräte** auf **Regeln anpassen**.

   Daraufhin wird das Fenster **Eigenschaften: Nicht zugeordnete Geräte** geöffnet.
3. Wählen Sie im Bereich **Geräte verschieben** die Regel für das Verschieben von Geräten, die Sie klonen möchten.
4. Klicken Sie auf die Schaltfläche **Klonregel**.

Ein Klon der ausgewählten Regel für das Verschieben von Geräten wird zum Ende der Liste hinzugefügt.

Eine neue Regel wird im deaktivierten Zustand erstellt. Sie können die Regel jederzeit ändern und aktivieren.

Software-Kategorisierung

Das wichtigste Tool zur Kontrolle des Starts von Apps sind die *Kategorien von Kaspersky* (im Weiteren auch *KL-Kategorien*). Die KL-Kategorien erleichtern dem Administrator von Kaspersky Security Center die Aufrechterhaltung der Kategorisierung der Software und verringern den Umfang des Datenverkehrs, der an die verwalteten Geräte übergeben wird.

Benutzerdefinierte Kategorien müssen nur für Programme erstellt werden, die nicht unter eine KL-Kategorie fallen (beispielsweise für Programme, die auf Bestellung entwickelt wurden). Die benutzerdefinierten Kategorien werden auf der Grundlage der Programmpakete (MSI) oder auf der Grundlage des Ordners mit den Installationspaketen erstellt.

Falls es eine umfangreiche ergänzte Software-Sammlung gibt, die mithilfe der KL-Kategorien kategorisiert ist, kann es zweckmäßig sein, eine automatisch aktualisierte Kategorie zu erstellen. Eine solche Kategorie wird bei der Änderung des Ordners mit den Programmpaketen automatisch mit den Prüfsummen der ausführbaren Dateien ergänzt.

Erstellen Sie keine automatisch aktualisierten Programmkategorien für die folgenden Ordner: "Eigene Dateien", "%windir%', '%Programme%" und %Programme (x86)%. Die Dateien in diesen Ordnern ändern sich oft, was zur Erhöhung der Belastung auf den Administrationsserver und zur Erhöhung des Datenverkehres im Netzwerk führt. Es muss ein separater Ordner mit der Sammlung der Software erstellt und von Zeit zu Zeit ergänzt werden.

Erforderliche Bedingungen für die Installation von Programmen auf den Geräten des Kundenunternehmens

Der Prozess der Remote-Installation von Programmen Geräten des Kundenunternehmens stimmt mit dem Prozess der Remote-Installation von Programmen innerhalb des Unternehmens überein.

Zur Installation von Programmen auf den Geräten eines Kundenunternehmens müssen die folgenden Bedingungen erfüllt sein:

- Vor der Erstinstallation von Programmen auf den Geräten des Kundenunternehmens ist es erforderlich, den Administrationsagenten auf den Geräten zu installieren.

  Bei der Konfiguration des Installationspakets für den Administrationsagenten durch einen Dienstanbieter ist es erforderlich, im Eigenschaftenfenster des Installationspakets im Programm Kaspersky Security Center folgende Einstellungen anzupassen:

  - Geben Sie im Abschnitt **Verbindung** in der Zeile **Administrationsserver** dieselbe Adresse des virtuellen Administrationsservers wie bei der lokalen Installation des Administrationsagenten auf dem Verteilungspunkt an.

  - Aktivieren Sie im Abschnitt **Erweitert** das Kontrollkästchen **Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen**. Geben Sie in der Zeile **Adresse des Verbindungs-Gateways** die Adresse des Verteilungspunkts an. Als Adresse des Geräts können Sie die IP-Adresse oder den Namen des Geräts im Windows-Netzwerk angeben.

- Wählen Sie als Methode zum Laden des Installationspakets für den Administrationsagenten **Durch Ressourcen des Betriebssystems über Verteilungspunkte** aus. Die Auswahl der Methode zum Laden des Pakets erfolgt auf folgende Weise:

  - Bei der Installation von Programmen mit der Aufgabe zur Remote-Installation können Sie die Methode zum Laden des Installationspakets folgendermaßen auswählen:

    - Beim Erstellen der Aufgabe zur Remote-Installation im Fenster **Einstellungen**.

    - Im Eigenschaftenfenster der Aufgabe zur Remote-Installation im Abschnitt **Einstellungen**.

  - Bei der Installation von Programmen mit dem Assistenten für Remote-Installationen können Sie die Methode zum Laden des Installationspakets im Fenster des Assistenten **Einstellungen** auswählen.

- Das Benutzerkonto, das den Verteilungspunkt autorisiert, muss über Zugriff auf die Ressource "Admin$" auf allen Client-Geräten verfügen.

Lokale Einstellungen des Programms anzeigen und ändern

Die Verwaltung durch Kaspersky Security Center ermöglicht, lokale Programmeinstellungen auf Geräten über die Verwaltungskonsole im Remote-Betrieb zu verwalten.

Bei lokalen Programmeinstellungen handelt es sich um die Programmeinstellungen, die für ein Gerät individuell sind. Mit Kaspersky Security Center können Sie lokale Programmeinstellungen für Geräte bestimmen, die zu Administrationsgruppen gehören.

Einstellungen für Kaspersky-Anwendungen sind in den Handbüchern der jeweiligen Programme ausführlich beschrieben.

Um die lokalen Einstellungen eines Programms anzuzeigen oder zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Arbeitsbereich der Gruppe, zu welcher das gewünschte Gerät gehört, auf die Registerkarte **Geräte**.

2. Im Eigenschaftenfenster des Geräts im Abschnitt **Programme** wählen Sie das gewünschte Programm aus.

3. Öffnen Sie durch Doppelklick auf den Programmnamen oder durch Klicken auf die Schaltfläche **Eigenschaften** das Programmeigenschaftenfenster.

Daraufhin wird das Fenster mit den lokalen Einstellungen des gewählten Programms geöffnet, die Sie sich anzeigen lassen und geändert werden können.

Sie können die Einstellungen ändern, deren Änderung durch die Gruppenrichtlinie nicht gesperrt wird (Einstellungen, die in der Richtlinie nicht durch ein Schloss-Symbol (🔒) markiert sind).

Kaspersky Security Center und verwaltete Programme aktualisieren

Dieser Abschnitt beschreibt die einzelnen Schritte für das Update von Kaspersky Security Center und der verwalteten Programme.

Szenario: Datenbanken und Programme von Kaspersky regelmäßig aktualisieren

Dieser Abschnitt enthält ein Szenario zum regelmäßigen Update der Datenbanken, Softwaremodule und Anwendungen von Kaspersky. Nachdem Sie das Szenario "Netzwerkschutz konfigurieren" abgeschlossen haben, müssen Sie die Verlässlichkeit des Schutzsystems aufrecht erhalten, um sicherzustellen, dass die Administrationsserver und die verwalteten Geräte dauerhaft gegen verschiedene Bedrohungen wie Viren, Netzwerkangriffe und Phishing-Attacken geschützt sind.

Der Netzwerkschutz bleibt auf dem neuesten Stand, wenn folgende Komponenten regelmäßig aktualisiert werden:

- Kaspersky-Datenbanken und Programm-Module
- Installierte Kaspersky-Anwendungen, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen

Wenn Sie dieses Szenario abschließen, können Sie sicher sein, dass:

- Ihr Netzwerk durch die aktuellsten Programme von Kaspersky, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen, geschützt ist.
- die Antiviren-Datenbanken und andere, für die Sicherheit des Netzwerks kritische Kaspersky-Datenbanken, immer auf dem neuesten Stand sind.

Erforderliche Vorrausetzungen

Die verwalteten Geräte benötigen eine Verbindung zum Administrationsserver. Wenn sie keine Verbindung haben, erwägen Sie eine manuelle Aktualisierung der Datenbanken von Kaspersky, Programm-Module und Programme oder eine Aktualisierung direkt von den Kaspersky-Update-Servern.

Der Administrationsserver muss eine Verbindung zum Internet haben.

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

1. die Sicherheitsanwendungen von Kaspersky gemäß dem Szenario zur Verteilung von Kaspersky-Anwendungen via Kaspersky Security Center Web Console auf den verwalteten Geräten verteilt haben.
2. alle notwendigen Richtlinien, Richtlinienprofile und Aufgaben entsprechend dem Szenario "Konfiguration des Netzwerkschutzes" konfiguriert haben.
3. in Übereinstimmung mit der Anzahl der verwalteten Geräte und der Netzwerktopologie eine geeignete Anzahl an Verteilungspunkten zugewiesen haben.

Das Update der Datenbanken und Anwendungen von Kaspersky erfolgt in mehreren Schritten:

1. **Auswählen eines Update-Schemas**

   Es existieren verschiedene Schemas die Sie nutzen können, um Updates für die Komponenten des Kaspersky Security Centers und Sicherheitsanwendungen zu installieren. Wählen Sie ein Schema oder mehrere Schemas, welche die Anforderungen Ihres Netzwerks am besten erfüllen.

2. **Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen**

   Diese Aufgabe wird automatisch vom Schnellstartassistent des Kaspersky Security Centers erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe jetzt.

   Diese Aufgabe wird benötigt, um Updates von den Kaspersky-Update-Servern in die Datenverwaltung des Administrationsservers zu laden, und um die Updates der Kaspersky-Datenbanken und Programm-Module des Kaspersky Security Centers auszuführen. Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, werden die Updates aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte geladen. In diesem Fall laden die verwalteten Geräte, die sich im Bereich eines Verteilungspunktes befinden, die Updates aus der Datenverwaltung des Verteilungspunktes, anstatt aus der Datenverwaltung des Administrationsservers.

   Anleitung:

   - Verwaltungskonsole: Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen
   - Kaspersky Security Center Web Console: Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen

3. **Aufgabe zum Download von Updates in die Datenverwaltung auf Verteilungspunkte erstellen (optional)**

   Standardmäßig werden die Updates von den Verteilungspunkten vom Administrationsserver heruntergeladen. Sie können Kaspersky Security Center so konfigurieren, dass die Verteilungspunkte die Updates direkt von den Kaspersky-Update-Servern herunterladen. Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt und die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* erstellt wurde, laden die Verteilungspunkte Updates von den Kaspersky-Update-Servern herunter, und nicht von der Datenverwaltung des Administrationsservers.

   Anleitung:

   - Verwaltungskonsole: Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen
   - Kaspersky Security Center Web Console: Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

4. **Konfigurieren der Verteilungspunkte**

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, stellen Sie sicher, dass die Option **Updates verteilen** in den Einstellungen aller benötigten Verteilungspunkten aktiviert ist. Wenn diese Option für einen Verteilungspunkt deaktiviert ist, laden die Geräte, die sich im Bereich dieses Verteilungspunktes befinden, die Updates von der Datenverwaltung des Administrationsservers herunter.

   Wenn Sie möchten, dass verwaltete Geräte ihre Updates nur über Verteilungspunkte erhalten, aktivieren Sie die Option **Dateien nur über Verteilungspunkte übertragen** in der Richtlinie des Administrationsagenten.

5. **Optimieren des Update-Vorgangs durch die Nutzung des autonomen Modells für den Update-Download oder mithilfe von Diff-Dateien (optional)**

   Sie können den Prozesses durch die Nutzung des autonomen Modells für den Download von Updates (standardmäßig aktiviert) oder durch die Nutzung von Diff-Dateien optimieren. Für jedes Netzwerksegment müssen Sie eine der beiden Funktionen auswählen, da diese nicht simultan arbeiten können.

   Wenn das autonome Modell für den Download von Updates aktiviert ist, lädt der Administrationsagent die benötigten Updates auf das verwaltete Gerät. Dies geschieht, sobald die Updates in die Datenverwaltung des Administrationsservers geladen wurden und bevor die Sicherheitsanwendung die Updates anfragt. Dies erhöht die Verlässlichkeit des Update-Prozesses. Um diese Funktion zu nutzen, aktivieren Sie die Option **Updates und Antiviren-Datenbanken im Voraus vom Administrationsserver herunterladen (empfohlen)** in der Richtlinie des Administrationsagenten.

   Wenn Sie das autonome Modell für den Download von Updates nicht benutzen, können Sie den Datenverkehr zwischen Administrationsserver und verwalteten Geräten optimieren, indem Sie Diff-Dateien benutzen. Wenn diese Funktion aktiviert ist, laden der Administrationsserver oder ein Verteilungspunkt im Gegensatz zu ganzen Kaspersky-Datenbank-Dateien oder Programm-Modulen nur Diff-Dateien herunter. Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Deswegen benötigt eine Diff-Datei weniger Platz als eine ganze Datei. Dies resultiert in einem verringerten Datenverkehr zwischen dem Administrationsserver oder Verteilungspunkt und den verwalteten Geräten. Um diese Funktion zu nutzen, aktivieren Sie die Option **Diff-Dateien herunterladen** in den Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und/oder der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*.

   Anleitung:

   - Diff-Dateien zum Update von Kaspersky-Datenbanken und -Software-Modulen verwenden
   - Verwaltungskonsole: Autonomes Modell für den Download von Updates aktivieren und deaktivieren
   - Kaspersky Security Center Web Console: Autonomes Modell für den Download von Updates aktivieren und deaktivieren

6. **Heruntergeladene Updates prüfen (optional)**

   Bevor Sie heruntergeladene Updates installieren, können Sie diese mit der Aufgabe zur *Update-Prüfung* überprüfen. Diese Aufgabe führt die anhand von Einstellungen für die angegebene Sammlung von Testgeräten konfigurierten Aufgaben zum Geräte-Update und zur Schadsoftware-Untersuchung nacheinander aus. Nach Erhalt des Resultats der Aufgabe, startet oder blockiert der Administrationsserver die Verteilung der Updates auf die verbliebenen Geräte.

   Die Aufgabe zur *Update-Prüfung* kann im Rahmen der Aufgabe für den *Download von Updates in die Datenverwaltung des Administrationsservers* ausgeführt werden. Aktivieren Sie in der Verwaltungskonsole in den Einstellungen der Aufgabe zum *Download von Updates in die Datenverwaltung des Administrationsservers* die Option **Update-Prüfung vor der Verteilung ausführen** oder in der Kaspersky Security Center Web Console die Option **Update-Prüfung ausführen**.

   Anleitung:

   - Verwaltungskonsole: Heruntergeladene Updates prüfen
   - Kaspersky Security Center Web Console: Heruntergeladene Updates prüfen

7. **Genehmigen und Ablehnen von Software-Updates**

Standardmäßig besitzen heruntergeladene Software-Updates den Status *Nicht definiert*. Sie können den Status auf *Genehmigt* oder *Abgelehnt* ändern. Genehmigte Updates werden immer installiert. Wenn ein Update eine Überprüfung und ein Akzeptieren des Endbenutzer-Lizenzvertrags benötigt, müssen Sie die Bestimmungen zuerst akzeptieren. Danach kann das Update an die verwalteten Geräte verteilt werden. Die nicht definierten Updates können nur in Übereinstimmungen mit den Richtlinieneinstellungen des Administrationsagenten auf dem Administrationsagent und auf anderen Komponenten von Kaspersky Security Center installiert werden. Updates, für die Sie den Status *Abgelehnt* gewählt haben, werden auf den Geräten nicht installiert. Wenn ein abgelehntes Update für eine Sicherheitsanwendung bereits zuvor installiert wurde, wird Kaspersky Security Center versuchen, dieses Update von allen Geräten zu deinstallieren.

Das Genehmigen und Ablehnen von Updates ist nur für Administrationsagenten und verwaltete Kaspersky-Anwendungen verfügbar, die auf Windows- oder Linux-basierten Client-Geräten installiert sind. Eine nahtlose Aktualisierung wird von den folgenden Komponenten nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung.

Anleitung:

- Verwaltungskonsole: Genehmigen und Ablehnen von Programm-Updates
- Kaspersky Security Center Web Console: Genehmigen und Ablehnen von Programm-Updates

8. **Konfiguration der automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center**

   Die heruntergeladenen Updates und Patches für den Administrationsagenten und andere Komponenten von Kaspersky Security Center werden automatisch installiert. Wenn Sie die Option **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren** in den Einstellungen des Administrationsagenten aktiviert haben, werden alle Updates nach dem Herunterladen in die Datenverwaltung (oder in mehrere Datenverwaltungen) automatisch installiert. Wenn die Option deaktiviert ist, werden die Patches von Kaspersky, die heruntergeladen und mit dem Status *Nicht festgestellt* markiert sind, erst installiert, wenn Sie ihren Status auf *Genehmigt* ändern.

   Anleitung:

   - Verwaltungskonsole: Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren
   - Kaspersky Security Center Web Console: Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren

9. **Installation von Updates für den Administrationsserver**

   Programm-Updates für den Administrationsserver sind nicht vom Update-Status abhängig. Sie werden nicht automatisch installiert und müssen zunächst durch den Administrator auf der Registerkarte **Überwachung** in der Verwaltungskonsole (**Administrationsserver** `<Servername>` → **Überwachung**), oder in dem Abschnitt **Benachrichtigungen** in der Kaspersky Security Center Web Console (**Überwachung und Berichterstattung** → **Benachrichtigungen**) genehmigt werden. Danach muss der Administrator die Installation der Updates explizit ausführen.

10. **Konfiguration der automatischen Installation von Updates für die Sicherheitsanwendungen**

    Erstellen Sie die Aufgabe *Update* für verwaltete Programme, um zeitnahe Updates für die Anwendungen, Programm-Module und Kaspersky-Datenbanken (einschließlich der Antiviren-Datenbanken) zu gewährleisten. Um zeitnahe Updates zu gewährleisten, wird es empfohlen, dass Sie beim Konfigurieren des Aufgabenzeitplans die Option **Nach dem Download von Updates in die Datenverwaltung** auswählen.

    Wenn Ihr Netzwerk ausschließlich IPv6-Geräte enthält und Sie regelmäßig die auf den Geräten installierten Sicherheitsanwendungen aktualisieren wollen, stellen Sie sicher, das auf den verwalteten Geräten jeweils der Administrationsserver und der Administrationsagent ab der Version 13.2 installiert sind.

    Standardmäßig werden Updates für Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Security für Linux erst installiert, nachdem der Update-Status auf *Genehmigt* geändert wurde. Sie können die Update-Einstellungen in der Aufgabe *Update* ändern.

Wenn ein Update eine Überprüfung und ein Akzeptieren des Endbenutzer-Lizenzvertrags benötigt, müssen Sie die Bestimmungen zuerst akzeptieren. Danach kann das Update an die verwalteten Geräte verteilt werden.

Anleitung:

- Verwaltungskonsole: Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren
- Kaspersky Security Center Web Console: Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren

Ergebnisse

Bei Abschluss des Szenarios ist Kaspersky Security Center so konfiguriert, dass die Updates der Kaspersky-Datenbanken und installierten Kaspersky-Anwendungen ausgeführt werden, nachdem die Updates in die Datenverwaltung des Administrationsservers oder der Verteilungspunkte geladen werden. Anschließend können Sie mit der Überwachung des Netzwerkstatus fortfahren.

Über das Aktualisieren der Datenbanken, Software-Module und Programme von Kaspersky

Um sicherzustellen, dass der Schutz Ihrer Administrationsserver und verwalteten Geräte auf dem neuesten Stand ist, müssen Sie zeitnah Updates bereitstellen für:

- Kaspersky-Datenbanken und Programm-Module

  Vor dem Herunterladen von Kaspersky-Datenbanken und Softwaremodulen überprüft Kaspersky Security Center, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Dies ist erforderlich, um sicherzustellen, dass die Antiviren-Datenbanken aktualisiert werden und das Sicherheitsniveau für die verwalteten Geräte beibehalten wird.

- Installierte Kaspersky-Anwendungen, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen

  Kaspersky Security Center ermöglicht Ihnen die automatische Aktualisierung des Administrationsagenten und der Kaspersky-Anwendungen auf Geräten mit Windows und Linux. Ein nahtloses Update der folgenden Komponenten wird nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung. Um diese Komponenten zu aktualisieren, müssen Sie die jeweils aktuellste Version von der Kaspersky-Website herunterladen und anschließend manuell installieren.

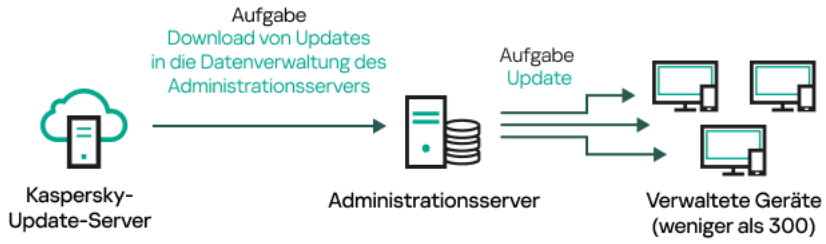
Abhängig von der Konfiguration Ihres Netzwerks können Sie die folgenden Schemata für das Herunterladen und Verteilen der erforderlichen Updates auf die verwalteten Geräte verwenden:

- Durch Verwendung einer einzelnen Aufgabe: *Download von Updates in die Datenverwaltung des Administrationsservers*
- Durch Verwendung zweier Aufgaben:
  - Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*
  - Die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*

- Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server
- Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security auf den verwalteten Geräten
- Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Verwenden der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers

In diesem Schema lädt Kaspersky Security Center über die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* Updates herunter. In kleinen Netzwerken, die weniger als 300 verwaltete Geräte in einem einzelnen Netzwerksegment oder weniger als 10 verwaltete Geräte in jedem Netzwerksegment enthalten, werden die Updates direkt aus der Datenverwaltung des Administrationsservers auf die verwalteten Geräte verteilt (siehe Abbildung unten).

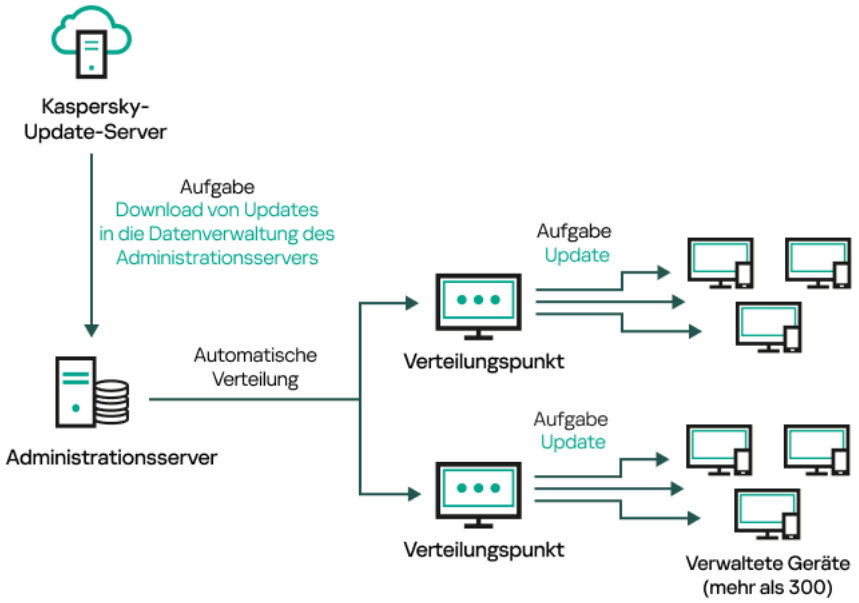


Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers ohne Verteilungspunkte

Standardmäßig verwendet der Administrationsserver zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können Administrationsserver so einrichten, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Wenn Ihr Netzwerk mehr als 300 verwaltete Geräte in einem einzigen Netzwerksegment enthält oder wenn Ihr Netzwerk aus mehreren Netzwerksegmenten mit mehr als 9 verwalteten Geräten in jedem Netzwerksegment besteht, empfehlen wir Ihnen, Verteilungspunkte zu verwenden, um die Updates auf die verwalteten Geräte zu übertragen (siehe Abbildung unten). Verteilungspunkte reduzieren die Belastung des Administrationsservers und optimieren den Datenverkehr zwischen dem Administrationsserver und den verwalteten Geräten. Sie können die Anzahl und Konfiguration der für Ihr Netzwerk benötigten Verteilungspunkte berechnen.

In diesem Schema werden die Updates automatisch aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte heruntergeladen. Die verwalteten Geräte, die zum Umfang eines Verteilungspunkts gehören, laden die Updates aus der Datenverwaltung des Verteilungspunkts anstelle der Datenverwaltung des Administrationsservers herunter.



Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers mit Verteilungspunkten

Wenn die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* abgeschlossen ist, werden die folgenden Updates in die Datenverwaltung des Administrationsservers heruntergeladen:

- Kaspersky-Datenbanken und Softwaremodule für Kaspersky Security Center

  Diese Updates werden automatisch installiert.

- Kaspersky-Datenbanken und Softwaremodule für die Sicherheitsanwendungen auf den verwalteten Geräten

  Diese Updates werden durch die Update-Aufgabe für Kaspersky Endpoint Security für Windows installiert.

- Updates für den Administrationsserver

  Diese Updates werden nicht automatisch installiert. Der Administrator muss die Installation der Updates ausdrücklich genehmigen und durchführen.

  > Für die Ins von Patches auf dem Administrationsserver sind lokale Administratorrechte erforderlich.

- Updates für die Komponenten von Kaspersky Security Center

  Standardmäßig werden diese Updates automatisch installiert. Sie können die Einstellungen in den Administrationsagent-Richtlinien ändern.

- Updates für die Sicherheitsanwendungen

  Standardmäßig installiert Kaspersky Endpoint Security für Windows nur die Updates, die Sie genehmigen (Die Updates können Sie über die Verwaltungskonsole oder über Kaspersky Security Center Web Console genehmigen). Die Updates werden mit der Aufgabe *Update* installiert und können in den Eigenschaften dieser Aufgabe konfiguriert werden.

Die Aufgabe zum *Download von Updates in die Datenverwaltung des Administrationsservers* steht auf virtuellen Administrationsservern nicht zur Verfügung. In der Datenverwaltung des virtuellen Administrationsservers werden Updates angezeigt, die auf den primären Administrationsserver heruntergeladen wurden.

Sie können die Updates, die auf Funktionsfähigkeit und Fehler geprüft werden sollen, auf einer Reihe von Testgeräten konfigurieren. Wenn die Überprüfung erfolgreich ist, werden die Updates an andere verwaltete Geräte verteilt.

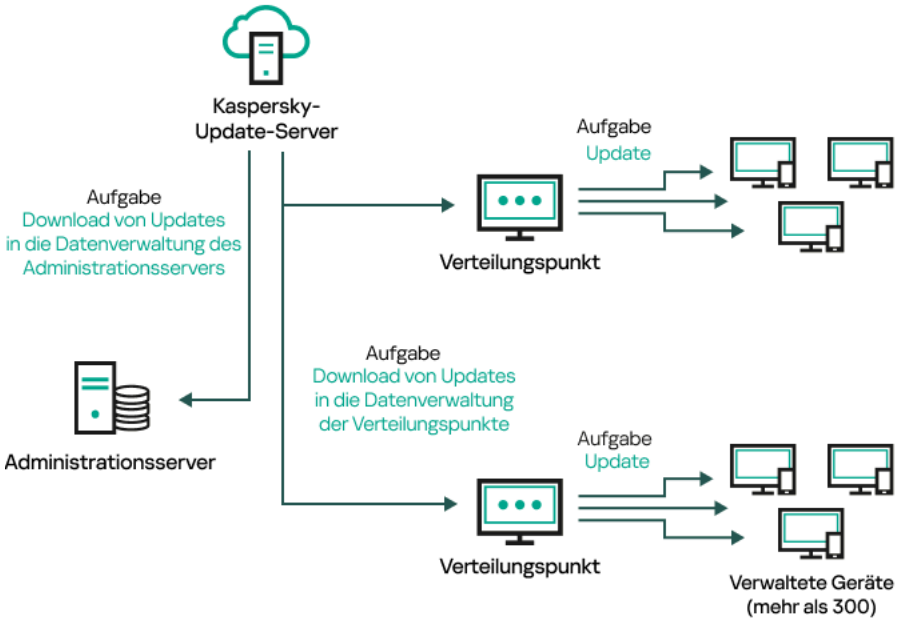
Jede Anwendung von Kaspersky fordert die erforderlichen Updates vom Administrationsserver an. Der Administrationsserver aggregiert diese Anforderungen und lädt nur die Aktualisierungen herunter, die von einer Anwendung angefordert werden. Dadurch wird sichergestellt, dass die gleichen Updates nicht mehrmals heruntergeladen werden und unnötige Updates überhaupt nicht heruntergeladen werden. Bei der Ausführung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* der Administrationsserver die folgenden Informationen automatisch an Kaspersky-Update-Server, um das Herunterladen von relevanten Versionen der Kaspersky-Datenbanken und Programm-Module sicherzustellen:

- Anwendungs-ID und Version des Programms
- ID der Programminstallation
- ID des aktiven Schlüssels
- Ausführungs-ID der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*

Keine der übermittelten Informationen enthält persönliche oder andere vertrauliche Daten. AO Kaspersky Lab schützt die erhaltenen Informationen in Übereinstimmung mit den geltenden gesetzlich festgelegten Anforderungen.

Verwendung von zwei Aufgaben: Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers und Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

Sie können Updates für die Datenverwaltungen der Verteilungspunkte direkt von den Update-Servern von Kaspersky anstelle der Datenverwaltung des Administrationsservers herunterladen und die Updates dann auf die verwalteten Geräte verteilen (siehe Abbildung unten). Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.



Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers und der Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

Standardmäßig verwenden der Administrationsserver und die Verteilungspunkte zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können den Administrationsserver und/oder die Verteilungspunkte so konfigurieren, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Um dieses Schema zu implementieren, erstellen Sie die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* zusätzlich zur Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*. Danach laden die Verteilungspunkte die Updates von den Kaspersky Update-Servern herunter und nicht von der Datenverwaltung des Administrationsservers.

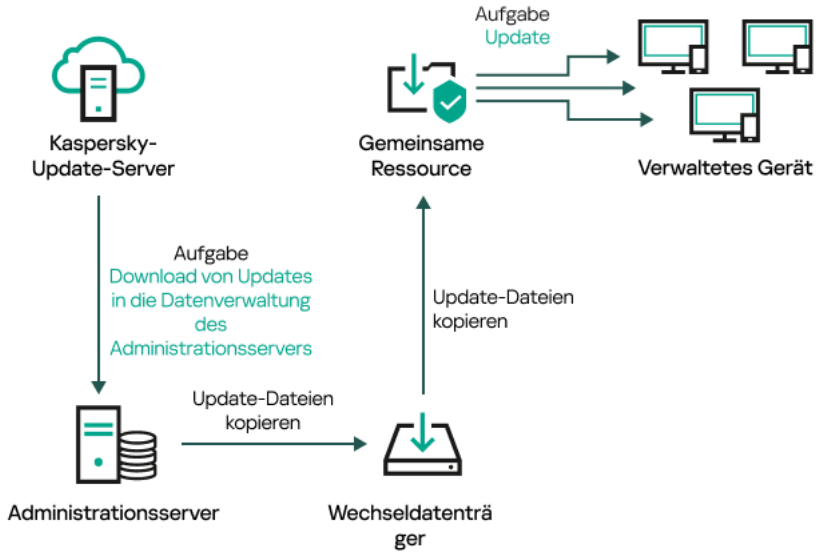
Geräte mit Verteilungspunkten unter macOS können keine Updates von Kaspersky Update-Servern herunterladen.

Wenn ein oder mehrere Geräte, die unter macOS laufen, in den Bereich der Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* fallen, schließt die Aufgabe mit dem Status *Fehlgeschlagen* ab, selbst wenn sie auf allen Windows-Geräten erfolgreich abgeschlossen wurde.

Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* wird auch für dieses Schema benötigt, da mit dieser Aufgabe Datenbanken und Softwaremodule von Kaspersky für das Kaspersky Security Center heruntergeladen werden können.

Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Wenn die Client-Geräte keine Verbindung zum Administrationsserver haben, können Sie einen lokalen Ordner oder eine freigegebene Ressource als Quelle für das Update von Kaspersky-Datenbanken, -Softwaremodulen und -Anwendungen verwenden. In diesem Schema müssen Sie die erforderlichen Updates aus der Datenverwaltung des Administrationsservers auf einen Wechseldatenträger und dann in den lokalen Ordner oder die als Update-Quelle in den Einstellungen von Kaspersky Endpoint Security angegebene freigegebene Ressource kopieren (siehe Abbildung unten).



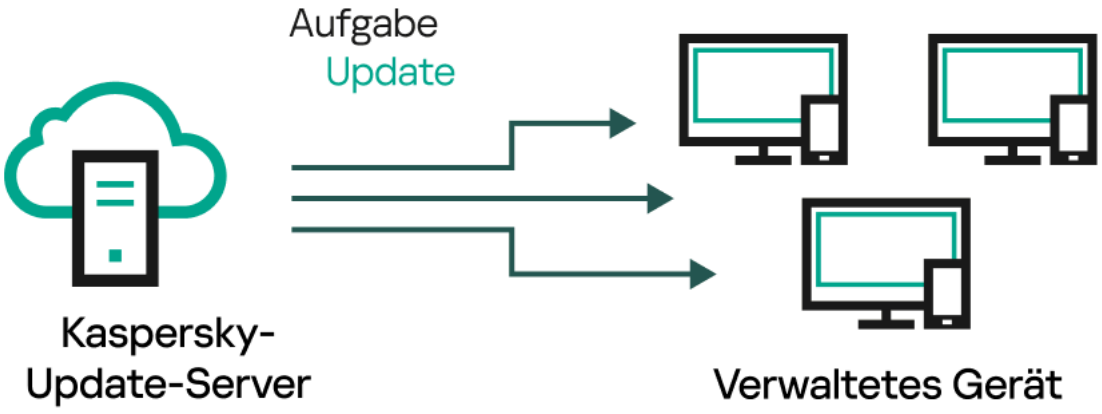
Manuelles Upgrade über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Weitere Informationen zu Update-Quellen in Kaspersky Endpoint Security finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux

Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security auf den verwalteten Geräten

Auf den verwalteten Geräten können Sie Kaspersky Endpoint Security so konfigurieren, dass Updates direkt von den Updateservern von Kaspersky empfangen werden (siehe Abbildung unten).



Updates von Sicherheitsanwendungen direkt von Kaspersky Update-Servern aus

In diesem Schema verwendet die Sicherheitsanwendung nicht die vom Kaspersky Security Center bereitgestellten Datenverwaltungen. Um Updates direkt von den Update-Servern von Kaspersky zu erhalten, geben Sie in der Schnittstelle der Sicherheitsanwendung die Update-Server von Kaspersky als Update-Quelle an. Weitere Informationen zu diesen Einstellungen finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux

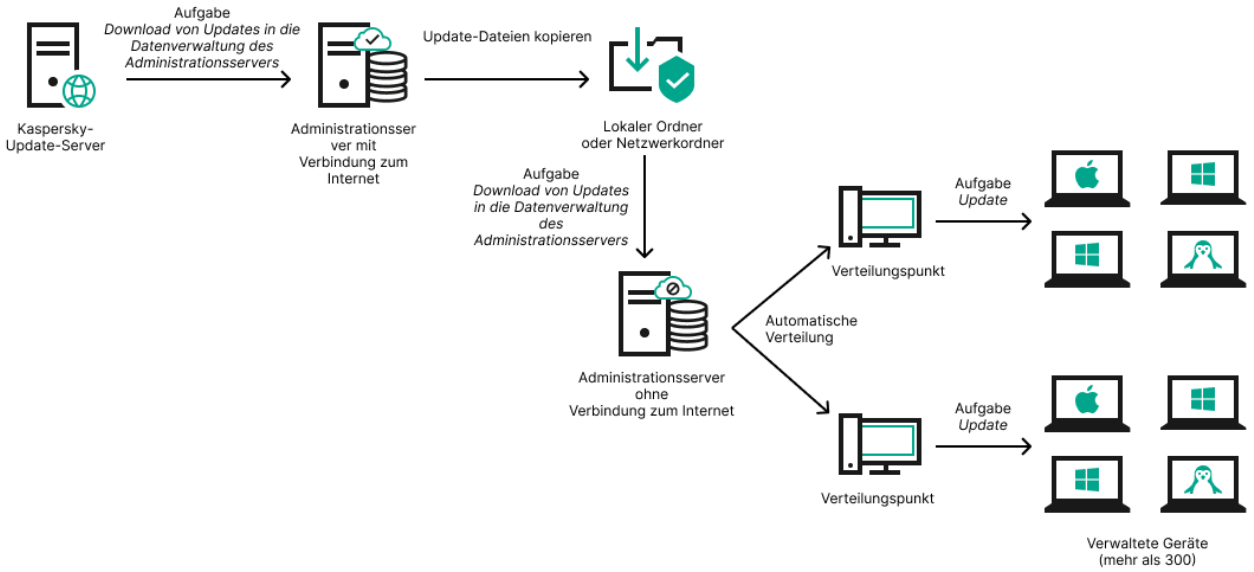
Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Wenn der Administrationsserver keine Internetverbindung hat, können Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zum Herunterladen von Updates aus einem lokalen oder Netzwerkordner konfigurieren. In diesem Fall müssen Sie die erforderlichen Update-Dateien von Zeit zu Zeit in den angegebenen Ordner kopieren. Beispielsweise können Sie die erforderlichen Update-Dateien aus einer der folgenden Quellen kopieren:

- Administrationsserver mit Internetverbindung (siehe Abbildung unten)

  Da ein Administrationsserver nur die Updates herunterlädt, die von den Sicherheitsanwendungen angefordert werden, müssen die Gruppen der Sicherheitsanwendungen, die von den Administrationsservern verwaltetet werden – d. h. von dem mit Internetverbindung und dem ohne Internetverbindung – übereinstimmen.

  Wenn der von Ihnen zum Herunterladen von Updates verwendete Administrationsserver die Version 13.2 besitzt, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option **Updates nach altem Schema herunterladen**.



Aktualisieren mittels eines lokalen Ordners oder Netzwerkordners, wenn der Administrationsserver keine Internetverbindung hat

- Kaspersky Update Utility

  Da dieses Tool das alte Schema zum Herunterladen von Updates verwendet, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option **Updates nach altem Schema herunterladen**.

Über die Verwendung von Diff-Dateien zum Update von Kaspersky-Datenbanken und Software-Modulen

Beim Download von Updates von den Kaspersky-Update-Servern entlastet Kaspersky Security Center den Datenverkehr durch die Verwendung von Diff-Dateien. Sie können festlegen, dass Geräte (Administrationsserver, Verteilungspunkte, Client-Geräte), die Updates von anderen Geräten in Ihrem Netzwerk erhalten, ebenfalls Diff-Dateien verwenden.

Über die Funktion zum Download von Diff-Dateien

Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Die Verwendung von Diff-Dateien entlastet den Datenverkehr in Ihrem Unternehmensnetzwerk, da Diff-Dateien weniger Platz einnehmen als die vollständigen Dateien der Datenbanken und Software-Module. Wenn die Funktion *Diff-Dateien herunterladen* auf dem Administrationsserver oder dem Verteilungspunkt aktiviert ist, werden die Diff-Dateien auf diesem Administrationsserver oder Verteilungspunkt gespeichert. So können Geräte, die Updates vom Administrationsserver oder einem Verteilungspunkt erhalten, die gespeicherten Diff-Dateien verwenden, um ihre Datenbanken und Software-Module zu aktualisieren.

Um die Verwendung von Diff-Dateien zu optimieren, wird empfohlen, den Update-Zeitplan der Geräte mit dem Update-Zeitplan des Administrationsservers oder dem Verteilungspunkt, von denen sie ihre Updates erhalten, zu synchronisieren. Der Datenverkehr kann jedoch auch dann reduziert werden, wenn die Geräte viel seltener aktualisiert werden als der Administrationsserver oder der Verteilungspunkt, von dem sie ihre Updates erhalten.

Die Funktion zum Download von Diff-Dateien kann nur auf Administrationsservern und Verteilungspunkten ab Version 11 aktiviert werden. Um Diff-Dateien auf älteren Versionen des Administrationsservers oder der Verteilungspunkte zu speichern, aktualisieren Sie diese mindestens auf die Version 11.

Die Funktion zum Download von Diff-Dateien ist nicht mit dem autonomen Modell für den Download von Updates kompatibel. Das bedeutet, dass Administrationsagenten, die das autonome Modell für den Download von Updates nutzen, keine Diff-Dateien herunterladen, selbst wenn die Funktion zum Download von Diff-Dateien auf dem Administrationsserver oder dem Verteilungspunkt, der Updates an diesen Administrationsagenten zustellt, aktiviert ist.

Verteilungspunkte verwenden kein IP-Multicast zur automatischen Verteilung von Diff-Dateien.

Funktion zum Herunterladen von Diff-Dateien aktivieren

Erforderliche Vorrausetzungen

Für dieses Szenario gelten folgende Voraussetzungen:

- Die Administrationsserver und Verteilungspunkte wurden auf Version 11 oder höher aktualisiert.
- Das autonome Modell für den Download von Updates wurde in den Einstellungen der Richtlinie des Administrationsagenten deaktiviert.

Schritte

1. **Aktivieren der Funktion auf dem Administrationsserver**

   Aktivieren Sie die Funktion in den Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers.

2. **Aktivieren der Funktion für einen Verteilungspunkt**

Aktivieren Sie die Funktion für Verteilungspunkte, die Updates mithilfe der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erhalten.

Aktivieren Sie anschließend die Funktion für Verteilungspunkte, die Updates vom Administrationsserver erhalten.

Die Funktion wird in den Einstellungen des Administrationsagenten und – falls die Verteilungspunkte manuell zugewiesen werden und Sie die Einstellungen der Richtlinie überbrücken möchten – im Abschnitt **Verteilungspunkte** in den Eigenschaften des Administrationsservers aktiviert.

Um zu prüfen, ob die Funktion zum Download von Diff-Dateien erfolgreich aktiviert wurde, können Sie den internen Datenverkehr vor und nach der Implementierung des Szenarios messen.

Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen

Die Administrationsserver-Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* wird automatisch bei der Ausführung des Schnellstartassistenten für Kaspersky Security Center erstellt. Die Aufgabe zum *Download von Updates in die Datenverwaltung des Administrationsservers* kann nur einmal erstellt werden. Deshalb können Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* nur dann erstellen, wenn sie aus der Liste mit Aufgaben des Administrationsservers entfernt wurde.

Gehen Sie wie folgt vor, um eine Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers zu erstellen:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Arten:
   - Wählen Sie in der Konsolenstruktur im Kontextmenü des Ordners **Aufgaben** den Punkt **Neu → Aufgabe** aus.
   - Klicken Sie im Arbeitsbereich des Ordners **Aufgaben** auf die Schaltfläche **Aufgabe erstellen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie auf der Seite **Aufgabentyp auswählen** des Assistenten die Option **Download von Updates in die Datenverwaltung des Administrationsservers**.
4. Legen Sie auf der Seite **Einstellungen** des Assistenten die Aufgabeneinstellungen wie folgt fest:
   - **Quellen der Updates**

     Als Update-Quelle für den Administrationsserver können die folgenden Ressourcen verwendet werden:

     - Kaspersky-Update-Server

       HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen. Standardmäßig verwendet der Administrationsserver zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können Administrationsserver so einrichten, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

       Standardmäßig ausgewählt.

     - Primärer Administrationsserver

       Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.

- Lokaler Ordner oder Netzwerkordner

  Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Ein Netzwerkordner kann ein FTP- oder HTTP-Server oder eine SMB-Freigabe sein. Für Netzwerkordner, die eine Authentifizierung erfordern, wird nur das SMB-Protokoll unterstützt. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

  Ein FTP- oder HTTP-Server oder ein Netzwerkordner, der von einer Update-Quelle verwendet wird, muss eine Ordnerstruktur (mit Updates) enthalten, die der Struktur entspricht, die bei Verwendung der Kaspersky-Update-Server erstellt wurde.

- **Sonstige Einstellungen**:

  - **Update der sekundären Administrationsserver erzwingen**

    Wenn diese Option aktiviert ist, startet der Administrationsserver die Update-Aufgaben auf den sekundären Administrationsservern sobald neue Updates heruntergeladen werden. Update-Aufgaben werden unter Verwendung der Update-Quellen gestartet, die in den Aufgabeneigenschaften auf den sekundären Administrationsservern konfiguriert ist.

    Wenn diese Option deaktiviert ist, werden die Update-Aufgaben auf den sekundären Administrationsservern gemäß ihren Zeitplänen gestartet.

    Diese Option ist standardmäßig deaktiviert.

  - **Heruntergeladene Updates in zusätzliche Ordner kopieren**

    Nachdem der Administrationsserver Updates empfängt, kopiert er sie in die angegebenen Ordner. Verwenden Sie diese Option, wenn Sie die Verteilung von Updates in Ihrem Netzwerk manuell verwalten möchten.

    Sie können diese Option beispielsweise in der folgenden Situation verwenden: Das Netzwerk Ihres Unternehmens besteht aus mehreren unabhängigen Subnetzen, wobei Geräte in den einzelnen Subnetzen über keinen Zugriff auf andere Subnetze verfügen. Allerdings haben Geräte in allen Teilnetzen Zugriff auf eine gemeinsame Netzwerkfreigabe. In diesem Fall müssen Sie den Administrationsserver in einem der Subnetze einrichten, um Updates von den Kaspersky-Update-Servern herunterzuladen. Aktivieren Sie diese Option und geben Sie dann diese Netzwerkfreigabe an. Geben Sie bei heruntergeladenen Updates der Repository-Aufgaben für andere Administrationsserver die gleiche Netzwerkfreigabe wie für die Update-Quelle an.

    Wenn Sie auswählen, dass die Updates in einen lokalen Ordner kopiert werden sollen, müssen Sie einen Ordner auf dem Gerät mit dem installierten Administrationsserver angeben. Der Pfad des Ordners hängt vom Betriebssystem auf dem Gerät ab. Da sich der lokale Ordner auf einem Linux-basierten Administrationsserver befindet, müssen Sie den POSIX-Pfad angeben. Beispiel: /Pfad/zum/Verzeichnis.

    Wenn Sie einen Netzwerkordner auswählen, der sich auf einem Linux-Administrationsserver befindet, müssen Sie vorher durch das Mounten des Ordners sicherstellen, dass von dem Gerät mit installiertem Administrationsserver auf den Netzwerkordner zugegriffen werden kann. Der Zugriff auf den Ordner erfolgt über das SMB-Protokoll.

    Diese Option ist standardmäßig deaktiviert.

    - **Update der Geräte und sekundären Administrationsserver bis Abschluss des Kopierens nicht erzwingen**

      Die Aufgaben zum Herunterladen von Updates auf Client-Geräte und sekundäre Administrationsserver werden erst gestartet, nachdem diese Updates vom Update-Hauptordner in die zusätzlichen Ordner kopiert wurden.

Diese Option muss aktiviert sein, wenn Client-Geräte und sekundäre Administrationsserver Updates von zusätzlichen Netzwerkordnern herunterladen.

Diese Option ist standardmäßig deaktiviert.

- **Updates nach altem Schema herunterladen**

  Ab Version 14 lädt Kaspersky Security Center die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit das Programm die Updates mittels des neuen Schemas herunterladen kann, muss die Update-Quelle die Updatedateien mitsamt den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Update-Quelle die Update-Dateien nur mit den Metadaten enthält, die ausschließlich mit dem alten Schema kompatibel sind, aktivieren Sie die Option **Updates nach altem Schema herunterladen**. Andernfalls schlägt die Aufgabe zum Update-Download fehl.

  Sie müssen diese Option beispielsweise aktivieren, wenn als Update-Quelle ein lokaler Ordner oder ein Netzwerkordner angegeben wurden, und wenn die Updatedateien in diesem Ordner von einer der folgenden Anwendungen heruntergeladen wurden:

  - Kaspersky Update Utility

    Dieses Tool lädt Updates unter Verwendung des alten Schemas herunter.

  - Kaspersky Security Center 13.2 oder frühere Version

    Beispiel: Ihr Administrationsserver 1 besitzt keine Internetverbindung. In diesem Fall können Sie Updates über einen 2. Administrationsserver herunterladen, welcher über eine Internetverbindung verfügt, und welcher die Updates anschließend in einem lokalen Ordner oder Netzwerkordner ablegt. Dieser dient wiederum als Update-Quelle für den 1. Administrationsserver. Wenn der Administrationsserver 2 mit Version 13.2 oder früher läuft, aktivieren Sie die Option **Updates nach altem Schema herunterladen** in der Aufgabe für Administrationsserver 1.

  Diese Option ist standardmäßig deaktiviert.

5. Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **Start nach Zeitplan**

     Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

     - **Alle n Stunden**

       Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

       Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

     - **Alle n Tage**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

       Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

     - **Alle n Wochen**

       Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

       Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

- **Alle n Minuten**

  Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

  Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

6. Geben Sie auf der Seite **Aufgabenname festlegen** des Assistenten den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

7. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

   Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nachdem der Assistent beendet ist, wird **Download von Updates in die Datenverwaltung des Administrationsservers** in der Liste der Aufgaben des Administrationsservers im Arbeitsbereich angezeigt.

Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Nach Fertigstellung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* werden die Datenbanken-Updates und Updates der Programm-Module von der Update-Quelle geladen und im freigegebenen Ordner des Administrationsservers gespeichert. Wenn die Aufgabe für eine Administrationsgruppe erstellt wird, kommt sie nur auf Administrationsagenten zur Anwendung, die zur angegebenen Administrationsgruppe gehören.

Updates werden aus dem gemeinsamen Ordner des Administrationsservers an Client-Geräte und sekundäre Administrationsserver verteilt.

Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

Geräte mit Verteilungspunkten unter macOS können keine Updates von Kaspersky Update-Servern herunterladen.

Wenn ein oder mehrere Geräte, die unter macOS laufen, in den Bereich der Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* fallen, schließt die Aufgabe mit dem Status *Fehlgeschlagen* ab, selbst wenn sie auf allen Windows-Geräten erfolgreich abgeschlossen wurde.

Sie können die Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* für eine Administrationsgruppe erstellen. Diese Aufgabe wird für die Verteilungspunkte ausgeführt, die zur angegebenen Administrationsgruppe gehören.

Sie können diese Aufgabe zum Beispiel dann nutzen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat. Wenn der Verteilungspunkt über einen Proxyserver mit dem Internet verbunden ist, müssen Sie die entsprechenden Einstellungen in der Richtlinie des Administrationsagenten angeben.

Um eine Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte für eine ausgewählte Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Starten Sie mithilfe der Schaltfläche **Neue Aufgabe** im Arbeitsbereich des Ordners den Assistenten für die Erstellung von Aufgaben.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie auf der Seite **Aufgabentyp auswählen** des Assistenten den Knoten **Kaspersky Security Center Administrationsserver** aus, erweitern Sie den Ordner **Erweitert** und wählen Sie dann die Aufgabe **Updates in die Datenverwaltung der Verteilungspunkte herunterladen** aus.

4. Legen Sie auf der Seite **Einstellungen** des Assistenten die Aufgabeneinstellungen wie folgt fest:

   - **Quellen der Updates**

     Als Update-Quelle für den Verteilungspunkt können die folgenden Ressourcen verwendet werden:

     - Kaspersky-Update-Server

       HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen.

       Diese Variante ist standardmäßig festgelegt.

     - Lokaler Ordner oder Netzwerkordner

       Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Ein Netzwerkordner kann ein FTP- oder HTTP-Server oder eine SMB-Freigabe sein. Für Netzwerkordner, die eine Authentifizierung erfordern, wird nur das SMB-Protokoll unterstützt. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

       > Ein FTP- oder HTTP-Server oder ein Netzwerkordner, der von einer Update-Quelle verwendet wird, muss eine Ordnerstruktur (mit Updates) enthalten, die der Struktur entspricht, die bei Verwendung der Kaspersky-Update-Server erstellt wurde.

   - **Ordner zum Speichern von Updates**

     Der Pfad zum angegebenen Ordner, in dem die bezogenen Updates gespeichert werden. Sie können den Pfad des angegebenen Ordners in die Zwischenablage kopieren. Für eine Gruppenaufgabe können Sie den Pfad eines angegebenen Ordners nicht ändern.

   - **Updates nach altem Schema herunterladen**

     Ab Version 14 lädt Kaspersky Security Center die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit die Anwendung die Updates mithilfe des neuen Schemas herunterladen kann, muss die Update-Quelle die Update-Dateien mit den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Update-Quelle die Update-Dateien mit Metadaten enthält, die nur mit dem alten Schema kompatibel sind, aktivieren Sie die Option **Updates nach altem Schema herunterladen**. Andernfalls schlägt die Aufgabe zum Update-Download fehl.

Sie müssen diese Option beispielsweise aktivieren, wenn als Update-Quelle ein lokaler Ordner oder ein Netzwerkordner angegeben sind, und wenn die Updatedateien in diesem Ordner von einer der folgenden Anwendungen heruntergeladen wurden:

- Kaspersky Update Utility

  Dieses Tool lädt Updates unter Verwendung des alten Schemas herunter.

- Kaspersky Security Center 13.2 oder frühere Version

  Ein Verteilungspunkt kann beispielsweise so konfiguriert sein, dass er die Updates aus einem lokalen oder aus einem Netzwerkordner übernimmt. In diesem Fall können Sie Updates über einen Administrationsserver mit Internetverbindung herunterladen und die Updates anschließend im lokalen Ordner des Verteilungspunkts ablegen. Wenn der Administrationsserver in Version 13.2 oder früher ausgeführt wird, aktivieren Sie in der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* die Option **Updates nach altem Schema herunterladen**.

Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf der Seite **Administrationsgruppe auswählen** des Assistenten auf **Durchsuchen** und wählen Sie die Administrationsgruppe aus, auf welche die Aufgabe verteilt wird.

6. Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **Start nach Zeitplan:**

     Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

     - **Alle n Stunden**

       Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

       Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

     - **Alle n Tage**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

       Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

     - **Alle n Wochen**

       Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

       Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

     - **Alle n Minuten**

       Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

       Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

7. Geben Sie auf der Seite **Aufgabenname festlegen** des Assistenten den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

8. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

   Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nachdem der Assistent abgeschlossen wurde, erscheint **Updates in die Datenverwaltung der Verteilungspunkte herunterladen** in der Aufgabenliste des Administrationsagenten in der Ziel-Administrationsgruppe und im Arbeitsbereich **Aufgaben** der Konsole.

Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Bei der Ausführung der Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* werden die Datenbanken-Updates und Updates der Programm-Module aus der Update-Quelle heruntergeladen und im freigegebenen Ordner gespeichert. Die heruntergeladenen Updates werden nur von jenen Verteilungspunkten verwendet, die zur angegebenen Administrationsgruppe gehören und für die keine separate Aufgabe zum Update-Download festgelegt wurde.

Wählen Sie im Fenster "Eigenschaften des Administrationsservers" im Bereich **Abschnitte** die Option **Verteilungspunkte** aus. In den Eigenschaften jedes Verteilungspunktes können Sie im Bereich **Update-Quellen** die Update-Quelle angeben (**Vom Administrationsserver beziehen** oder **Aufgabe zum erzwungenen Download von Updates verwenden**). Für einen Verteilungspunkt, der manuell oder automatisch zugewiesenen ist, ist standardmäßig die Variante **Vom Administrationsserver beziehen** ausgewählt. Solche Verteilungspunkte verwenden die Ergebnisse der Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte*.

In den Eigenschaften jedes Verteilungspunkts ist der Netzwerkordner angegeben, der individuell für diesen Verteilungspunkt konfiguriert ist. Die Namen der Ordner können sich je nach Verteilungspunkt unterscheiden. Deshalb wird nicht empfohlen, den Netzwerkordner der Updates in den Eigenschaften der Aufgabe, wenn die Aufgabe für eine Gruppe von Geräten erstellt wird.

Sie können den Netzwerkordner der Updates in den Eigenschaften der Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* bearbeiten, wenn Sie eine lokale Aufgabe für das Gerät erstellen.

Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers anpassen

Gehen Sie wie folgt vor, um eine Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers anzupassen:

1. Wählen Sie im Arbeitsbereich des Ordners **Aufgaben** der Konsolenstruktur die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** in der Aufgabenliste aus.

2. Öffnen Sie das Eigenschaftenfenster der Aufgabe auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf den Link **Aufgabe konfigurieren** im Informationsfeld der ausgewählten Datei.

   Daraufhin wird das Eigenschaftenfenster der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* geöffnet. Hier können Sie die Einstellungen für das Herunterladen von Updates in die Datenverwaltung des Administrationsservers anpassen.

Heruntergeladene Updates prüfen

Bevor Sie Updates auf den verwalteten Geräten installieren, können Sie die Updates zunächst über die Aufgabe *Update-Prüfung* auf Funktionsfähigkeit und Fehler überprüfen. Die Aufgabe *Update-Prüfung* wird im Rahmen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* automatisch ausgeführt. Der Administrationsserver lädt Updates aus der Quelle herunter, speichert sie in einem temporären Verzeichnis und startet die Aufgabe *Update-Prüfung*. Wenn die Aufgabe erfolgreich ausgeführt wurde, werden die Updates von der temporären Datenverwaltung in den freigegebenen Ordner des Administrationsservers (<Kaspersky Security Center-Installationsordner>\Share\Updates) kopiert. Sie werden an alle Client-Geräte verteilt, für die der Administrationsserver als Update-Quellen dient.

Wenn in den Ergebnissen der Aufgabe zur *Update-Prüfung* die im temporären Verzeichnis liegenden Updates als fehlerhaft eingestuft werden oder wenn die Aufgabe zur *Update-Prüfung* mit einem Fehler beendet wird, werden die Updates nicht im freigegebenen Ordner gespeichert. Auf dem Administrationsserver verbleibt das vorherige Update. Dann werden auch die Aufgaben mit dem Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** nicht gestartet. Diese Vorgänge werden beim nächsten Ausführen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* gestartet, wenn die Prüfung der neuen Updates erfolgreich verläuft.

Das Update gilt als fehlerhaft, wenn mindestens ein Testgerät eine der folgenden Bedingungen erfüllt:

- Es ist ein Fehler in einer Update-Aufgabe aufgetreten.
- Nach Übernahme der Updates hat sich der Status des Echtzeitschutzes der Sicherheitsanwendung geändert.
- Während der Ausführung der Untersuchungsaufgabe auf Befehl wurde ein infiziertes Objekt gefunden.
- Es ist ein Funktionsfehler einer Kaspersky-Anwendung aufgetreten.

Wenn auf keinem Testgerät eine der genannten Bedingungen erfüllt wurde, wird diese Updates als zulässig anerkannt und die Aufgabe *Update-Prüfung* gilt als erfolgreich abgeschlossen.

Bevor Sie mit der Erstellung der Aufgabe *Update-Prüfung* beginnen, führen Sie folgende Voraussetzungen aus:

1. Erstellen Sie eine Administrationsgruppe mit mehreren Testgeräten. Sie benötigen diese Gruppe, um mit ihr Updates zu prüfen.

   Es wird empfohlen Testgeräte zu verwenden, die gut geschützt sind und die eine Programmkonfiguration aufweisen, die im Unternehmensnetzwerk am weitesten verbreitet ist. Dieser Ansatz erhöht während der Untersuchung die Qualität und Wahrscheinlichkeit der Erkennung von Viren und minimiert das Risiko von Fehlalarmen. Wenn Viren auf Testgeräten gefunden werden, wird die Aufgabe zur *Update-Prüfung* als nicht erfolgreich betrachtet.

2. Erstellen Sie die Aufgaben *Update* und *Schadsoftware-Untersuchung* für ein von Kaspersky Security Center unterstütztes Programm, z. B. Kaspersky Endpoint Security für Windows oder Kaspersky Security für Windows Server. Geben Sie beim Erstellen der Aufgaben *Update* und *Schadsoftware-Untersuchung* die Administrationsgruppe mit den Testgeräten an.

   Die Aufgabe *Update-Prüfung* führt die Aufgaben *Update* und *Schadsoftware-Untersuchung* auf den Testgeräten nacheinander aus, um zu überprüfen, ob alle Updates zulässig sind. Beim Erstellen der Aufgabe *Update-Prüfung*, müssen Sie zusätzlich die Aufgaben *Update* und *Schadsoftware-Untersuchung* angeben.

3. Erstellen Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

Damit Kaspersky Security Center die abgerufenen Updates überprüft, bevor sie auf die Client-Geräte verteilt werden, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsbereich des Ordners **Aufgaben** die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* aus der Liste mit Aufgaben.

2. Öffnen Sie das Eigenschaftenfenster der Aufgabe auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

   - Klicken Sie im Informationsfeld der gewählten Aufgabe auf den Link **Aufgabeneinstellungen anpassen**.

3. Wenn die Aufgabe *Update-Prüfung* existiert, klicken Sie auf die Schaltfläche **Durchsuchen**. Wählen Sie im folgenden Fenster die Aufgabe *Update-Prüfung* in der Administrationsgruppe mit den Testgeräten aus.

4. Wenn Sie die Aufgabe *Update-Prüfung* noch nicht erstellt haben, klicken Sie auf die Schaltfläche **Erstellen**.

   Der Assistent für die Aufgabe *Update-Prüfung* wird gestartet. Folgen Sie den Anweisungen des Assistenten.

5. Klicken Sie auf **OK**, um das Eigenschaftenfenster der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zu schließen.

Die automatische Update-Prüfung ist aktiviert. Wenn Sie jetzt die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen, beginnt diese mit der Update-Prüfung.

Konfiguration der Prüfungsrichtlinien und Hilfsaufgaben

Beim Erstellen einer Aufgabe zur *Update-Prüfung* legt der Administrationsserver Prüfungsrichtlinien, zusätzliche Gruppenaufgaben zum Update und zur Untersuchung auf Befehl an.

Die Durchführung von Hilfsgruppenaufgaben zum Update und zur Untersuchung auf Befehl kann einige Zeit in Anspruch nehmen. Diese Aufgaben werden im Rahmen der Aufgabe zur *Update-Prüfung* ausgeführt. Die Aufgabe zur *Update-Prüfung* wird im Rahmen der Aufgabe *Download von Updates in die Datenverwaltung* ausgeführt. Die Zeit, die für die Aufgabe *Download von Updates in die Datenverwaltung* benötigt wird, umfasst auch die Zeit für unterstützende Gruppenaufgaben für Updates und die Untersuchung auf Befehl.

Die Einstellungen für die Prüfungsrichtlinien und Hilfsaufgaben können geändert werden.

Um die Einstellungen der Prüfungsrichtlinie oder einer Hilfsaufgabe zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum die Gruppe, für welche die Aufgabe zur *Update-Prüfung* erstellt wurde.
2. Klicken Sie im Arbeitsbereich auf eine der folgenden Registerkarten:
   - **Richtlinien**, wenn Sie die Einstellungen der Prüfungsrichtlinie ändern möchten.
   - **Aufgaben**, wenn Sie die Einstellungen der Hilfsaufgabe ändern möchten.
3. Wählen Sie im Arbeitsbereich der Registerkarte die Richtlinie oder die Aufgabe, deren Einstellungen Sie ändern möchten.
4. Öffnen Sie das Eigenschaftenfenster dieser Richtlinie (Aufgabe) auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf die Richtlinie (Aufgabe), und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinie konfigurieren** (**Aufgabe konfigurieren**) im Informationsfeld der ausgewählten Richtlinie (Aufgabe).

Damit die Update-Prüfung korrekt erfolgen kann, müssen die Änderungen der Einstellungen der Prüfungsrichtlinien und Hilfsaufgaben unter folgenden Aspekten vorgenommen werden:

- In den Einstellungen für Hilfsaufgaben:
  - Es müssen alle Aufgaben der Ereigniskategorie **Kritisches Ereignis** und **Funktionsfehler** auf dem Administrationsserver gespeichert werden. Der Administrationsserver analysiert den Programmverlauf aufgrund von Ereignissen dieser Arten.
  - Als Update-Quelle muss der Administrationsserver verwendet werden.
  - Die Zeitplanart für die Aufgaben muss angegeben werden: **Manuell**.

- In den Einstellungen der Prüfungsrichtlinien:

  - Deaktivieren Sie die iChecker- und iSwift-Technologien zur Beschleunigung der Untersuchung (**Basisschutz → Schutz vor bedrohlichen Dateien → Einstellungen → Erweitert → Untersuchungstechnologien**).

  - Wählen Sie die Aktionen für infizierte Objekte aus: **Desinfizieren; löschen, wenn Desinfektion nicht möglich** / **Desinfizieren; blockieren, wenn Desinfektion nicht möglich** / **Blockieren**. (**Basisschutz → Schutz vor bedrohlichen Dateien → Aktion bei Bedrohungserkennung**).

- In den Einstellungen der Prüfungsrichtlinien und Hilfsaufgaben:

  Wenn nach der Installation der Updates für die Programm-Module ein Neustart des Geräts erforderlich ist, muss dieser unverzüglich ausgeführt werden. Wenn das Gerät nicht neu gestartet wird, kann die Richtigkeit dieses Typs von Updates nicht überprüft werden. Bei einigen Anwendungen kann die Installation der Updates, die einen Neustart erfordern, unterdrückt sein oder erst nach Bestätigung durch den Benutzer erfolgen. Diese Beschränkungen müssen in den Einstellungen der Prüfungsrichtlinien und Hilfsaufgaben deaktiviert sein.

Heruntergeladene Updates anzeigen

Um die Liste der heruntergeladenen Updates anzusehen,

Wählen Sie in der Konsolenstruktur aus dem Ordner **Datenverwaltung** den Unterordner **Updates für Kaspersky-Datenbanken und -Softwaremodule**.

Im Arbeitsbereich des Ordners **Updates für Kaspersky-Datenbanken und -Softwaremodule** wird eine Liste der Updates angezeigt, die auf dem Administrationsserver gespeichert sind.

Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren

Sie können das automatische Datenbanken-Update und das Update der Programm-Module von Kaspersky Endpoint Security auf den Client-Geräten konfigurieren.

Um den Download und die automatische Installation von Updates für Kaspersky Endpoint Security auf den Geräten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Erstellen Sie eine Aufgabe mit dem Typ **Update** auf eine der folgenden Arten:

   - Wählen Sie in der Konsolenstruktur aus dem Kontextmenü des Ordners **Aufgaben** den Punkt **Neu → Aufgabe** aus.

   - Klicken Sie Arbeitsbereich des Ordners **Aufgaben** auf **Neue Aufgabe**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie auf der Seite **Aufgabentyp auswählen** des Assistenten **Kaspersky Endpoint Security** als Aufgabentyp aus und wählen Sie dann **Update** als den Aufgabenuntertyp.

4. Folgen Sie den weiteren Schritten des Assistenten.

   Nach dem Abschluss des Assistenten wird eine Update-Aufgabe für Kaspersky Endpoint Security erstellt. Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsbereich des Ordners **Aufgaben** angezeigt.

5. Wählen Sie im Arbeitsbereich des Ordners **Aufgaben** die erstellte Update-Aufgabe aus.

6. Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

7. Wählen Sie im nächsten Fenster im Bereich **Abschnitte** den Punkt **Optionen** aus.

   Im Abschnitt **Optionen** können Sie die Einstellungen für die Update-Aufgabe im lokalen und mobilen Modus anpassen:

   - **Update-Einstellungen für lokalen Modus**: zwischen dem Gerät und Administrationsserver ist eine Verbindung hergestellt.

   - **Update-Einstellungen für mobilen Modus**: zwischen Kaspersky Security Center und dem Gerät besteht keine Verbindung (wenn beispielsweise das Gerät nicht mit dem Internet verbunden ist).

8. Mithilfe der Schaltfläche **Einstellungen** wählen Sie die Update-Quelle.

9. Aktivieren Sie die Option **Updates für Programm-Module herunterladen**, um die Updates für die Programm-Module gemeinsam mit den Programm-Datenbanken herunterzuladen und zu installieren.

   Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Endpoint Security den Benutzer über verfügbare Updates für Programm-Module und aktiviert während der Ausführung der Update-Aufgabe das Update der Programm-Module im Update-Paket. Passen Sie das Übernehmen der Updates durch die Module an:

   - **Kritische und genehmigte Updates installieren**. Wenn Updates für die Programm-Module verfügbar sind, installiert Kaspersky Endpoint Security Updates mit dem Status *Kritisch* automatisch; die restlichen Updates werden installiert, nachdem Sie diese genehmigt haben.

   - **Nur bestätigte Updates installieren**. Verfügbare Updates für Programm-Module von Kaspersky Endpoint Security werden installiert, nachdem die Installation entweder lokal über die Benutzeroberfläche des Programms oder über Kaspersky Security Center genehmigt wurde.

   Wenn für es für das Update von Programm-Modulen erforderlich ist, dass sich der Benutzer mit den Bedingungen des Lizenzvertrags und Datenschutzrichtlinie vertraut macht und diese akzeptiert, werden die Updates installiert, nachdem der Benutzer die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie akzeptiert hat.

10. Aktivieren Sie die Option **Updates in Ordner kopieren**, damit die Anwendung die heruntergeladenen Updates in einem Ordner speichert, und klicken Sie dann auf die Schaltfläche **Durchsuchen**, um den Ordner auszuwählen.

11. Klicken Sie auf die Schaltfläche **OK**.

Beim Ausführen der Aufgabe **Update** sendet das Programm Anfragen an die Kaspersky-Update-Server.

Einige Updates erfordern die Installation der neuesten Versionen von Verwaltungs-Plug-ins.

Autonomes Modell für den Download von Updates

Der Administrationsagent auf den verwalteten Geräten kann möglicherweise nicht immer eine Verbindung zum Administrationsserver herstellen, um Updates herunterzuladen. Ein Administrationsagent kann beispielsweise auf einem Notebook installiert sein, das manchmal nicht mit dem Internet oder dem lokalen Netzwerk verbunden ist. Außerdem kann der Administrator die Verbindungszeit der Geräte mit dem Netzwerk beschränken. In solchen Fällen können Geräte mit installiertem Administrationsagenten Updates vom Administrationsserver nicht nach Zeitplan herunterladen. Wenn ein Update eines verwalteten Programms (beispielsweise Kaspersky Endpoint Security) mithilfe eines Administrationsagenten konfiguriert wird, ist für das Update eine Verbindung zum Administrationsserver erforderlich. Kommt keine Verbindung zwischen Administrationsagent und Administrationsserver zustande, ist kein Update möglich. Die Verbindung zwischen Administrationsagent und Administrationsserver kann so konfiguriert sein, dass sich der Agent nur zu bestimmten Zeiten mit dem Server verbindet. Im schlechtesten Fall, wenn sich die festgelegten Verbindungsintervalle mit Zeiträumen überschneiden, zu denen keine Verbindung zustande kommt, werden die Datenbanken niemals aktualisiert. Ferner kann es zu Situationen kommen, in denen viele verwaltete Programme gleichzeitig auf den Administrationsserver zugreifen, um Updates herunterzuladen. In einem solchen Fall kann der Administrationsserver die Beantwortung von Anfragen einstellen (wie während eines DDoS-Angriffs).

Zur Vermeidung solcher Probleme verfügt Kaspersky Security Center über ein autonomes Modell für den Download von Datenbanken-Updates und Modulen der verwalteten Programme. Dieses Modell stellt einen Mechanismus zur Update-Verteilung unabhängig von vorübergehender Unzugänglichkeit der Übertragungskanäle des Administrationsservers bereit. Das Modell verringert ferner die Auslastung des Administrationsservers.

So funktioniert das autonome Modell für den Download von Updates

Wenn der Administrationsserver Updates empfängt, benachrichtigt der Administrationsagent (auf Geräten, auf denen er installiert ist) von den Updates, die für verwaltete Apps erforderlich sind. Wenn der Administrationsagent Informationen über diese Updates erhalten, ladet er die erforderlichen Dateien vom Administrationsserver im Voraus herunter. Bei der ersten Verbindung zum Administrationsagenten wird ein Updatedownload vom Administrationsserver initiiert. Nachdem der Administrationsagent alle Updates auf das Client-Gerät heruntergeladen hat, stehen die Updates den Programmen auf dem Gerät zur Verfügung.

Wenn ein verwaltetes Programm auf dem Client-Gerät versucht, auf den Administrationsagenten zuzugreifen, um Updates herunterzuladen, überprüft der Administrationsagent, ob er über alle erforderlichen Updates verfügt. Wurden die Updates nicht mehr als 25 Stunden vor der Anfrage des verwalteten Programms vom Administrationsserver abgerufen, stellt der Administrationsagent keine Verbindung zum Administrationsserver her, sondern stellt dem verwalteten Programm die Updates aus dem lokalen Cache bereit. Eine Verbindung mit dem Administrationsserver wird möglicherweise nicht hergestellt, wenn der Administrationsagent Updates für Programme auf Client-Geräten bereitgestellt, für die Updates jedoch keine Verbindung erforderlich ist.

Um die Auslastung auf dem Administrationsserver zu verteilen, stellt der Administrationsagent auf einem Gerät während des vom Administrationsserver festgelegten Zeitraums eine Verbindung mit dem Administrationsserver her und lädt die Updates herunter. Dieses Zeitintervall hängt von der Anzahl von Geräten mit installiertem Administrationsagenten, die Updates herunterladen, sowie von der Größe dieser Updates ab. Um die Auslastung auf dem Administrationsserver zu verringern, können Sie den Administrationsagenten als Verteilungspunkt verwenden.

Wenn das autonome Modell zum Herunterladen von Updates deaktiviert ist, werden Updates entsprechend dem Zeitplan der Aufgabe zum Update-Download verteilt.

Das autonome Modell für den Download von Updates ist standardmäßig aktiviert.

Das autonome Modell für den Download von Updates wird nur für verwaltete Geräte verwendet, auf denen die Aufgabe zum Abrufen von Updates durch verwaltete Geräte als Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** ausgewählt hat. Für andere verwaltete Geräte wird das Standardsystem zum Update-Download vom Administrationsserver in Echtzeit verwendet.

Es wird empfohlen, das autonome Modell für den Download von Updates in den Einstellungen der Richtlinien des Administrationsagenten der entsprechenden Administrationsgruppen in diesen Fällen zu deaktivieren: wenn laut Konfiguration der verwalteten Programme der Update-Download nicht vom Administrationsserver, sondern von den Kaspersky-Servern oder einem Netzwerkordner vorgenommen wird, und wenn dabei für die Aufgabe zum Update-Download der Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** ausgewählt ist.

Autonomes Modell für den Download von Updates aktivieren und deaktivieren

Es wird empfohlen, das autonome Modell für den Download von Updates nicht zu deaktivieren. Die Deaktivierung kann zu Störungen bei der Zustellung von Updates an die Geräte führen. In einigen Fällen wird der Experte des Technischen Supports von Kaspersky Ihnen eventuell empfehlen, das Kontrollkästchen **Updates und Antiviren-Datenbanken vom Administrationsserver vorab herunterladen** zu deaktivieren. In einem solchen Fall müssen Sie sicherstellen, dass die Aufgabe zum Update-Download für Kaspersky-Anwendungen eingerichtet ist.

Um das autonome Modell zum Abrufen von Updates für die Administrationsgruppe zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe, für die das autonome Modell zum Abrufen von Updates aktiviert werden soll.
2. Öffnen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien**.
3. Auf der Registerkarte **Richtlinien** wählen Sie die Richtlinie des Administrationsagenten aus.
4. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Richtlinie des Administrationsagenten geöffnet.
5. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Verwaltung von Patches und Updates** aus.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Updates und Antiviren-Datenbanken vom Administrationsserver vorab herunterladen (empfohlen)**, um das autonome Modell für den Download von Updates zu aktivieren oder zu deaktivieren.

   Das autonome Modell für den Download von Updates ist standardmäßig aktiviert.

Das autonome Modell für den Download von Updates wird daraufhin aktiviert oder deaktiviert.

Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center

Standardmäßig werden die heruntergeladenen Updates und Patches für die folgenden Programmkomponenten automatisch installiert:

- Administrationsagent für Windows
- Verwaltungskonsole
- iOS MDM-Server

Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center sind nur für Windows-Geräte verfügbar. Sie können die automatische Installation der Updates und Patches für diese Komponenten deaktivieren. In diesem Fall werden die heruntergeladenen Updates und Patches nur installiert, sobald Sie ihren Status zu *Genehmigt* ändern. Updates und Patches mit dem Status *Nicht festgestellt* werden nicht installiert.

Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren

Die automatische Installation der Updates für Komponenten von Kaspersky Security Center wird standardmäßig bei der Installation des Administrationsagenten auf dem Gerät aktiviert. Sie können diese bei der Installation des Administrationsagenten oder später mithilfe einer Richtlinie deaktivieren.

Um die automatische Installation der Updates für Komponenten von Kaspersky Security Center bei der lokalen Installation des Administrationsagenten auf dem Gerät zu deaktivieren, gehen Sie wie folgt vor:

1. Starten Sie die lokale Installation des Administrationsagenten auf dem Gerät.
2. Deaktivieren Sie im Schritt **Erweiterte Einstellungen** das Kontrollkästchen **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**.
3. Folgen Sie den Anweisungen des Assistenten.

Auf dem Gerät wird der Administrationsagent mit der deaktivierten automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center installiert. Sie können die automatische Installation später mithilfe einer der Richtlinie aktivieren.

Um die automatische Installation der Updates für Komponenten von Kaspersky Security Center bei der Installation des Administrationsagenten auf dem Gerät mittels Installationspaket zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Remote-Installation → Installationspakete** aus.
2. Wählen Sie im Kontextmenü des Pakets **Kaspersky Security Center Administrationsagent <Versionsnummer>** den Punkt **Eigenschaften** aus.
3. Deaktivieren Sie in den Eigenschaften des Installationspakets, im Abschnitt **Einstellungen** das Kontrollkästchen **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**.

Der Administrationsagent wird aus diesem Paket mit der deaktivierten automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center installiert. Sie können die automatische Installation später mithilfe einer der Richtlinie aktivieren.

Wenn bei der Installation des Administrationsagenten auf dem Gerät das Kontrollkästchen aktiviert (deaktiviert) war, können Sie die automatische Installation später mithilfe einer Richtlinie des Administrationsagenten deaktivieren (aktivieren).

Um die automatische Installation der Updates für Komponenten von Kaspersky Security Center mithilfe einer Richtlinie des Administrationsagenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe, für welche die automatische Installation von Updates und Patches aktiviert oder deaktiviert werden soll.
2. Öffnen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien**.
3. Auf der Registerkarte **Richtlinien** wählen Sie die Richtlinie des Administrationsagenten aus.
4. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Richtlinie des Administrationsagenten geöffnet.
5. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Verwaltung von Patches und Updates** aus.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**, um das automatische Aktualisieren und Patchen entsprechend an- bzw. abzuschalten.
7. Aktivieren Sie das Symbol Schloss für dieses Kontrollkästchen.

Die Richtlinie wird auf die ausgewählten Geräte angewendet und die automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center wird auf diesen Geräten aktiviert (deaktiviert).

Updates automatisch verteilen

Kaspersky Security Center erlaubt eine automatische Verteilung und Installation von Updates auf Client-Geräten und sekundären Administrationsservern.

Updates automatisch auf Client-Geräte verteilen

Damit Updates für das ausgewählte Programm direkt nach dem Update-Download in die Datenverwaltung des Administrationsservers automatisch auf die Client-Geräte verteilt werden, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die Client-Geräte verwaltet.
2. Erstellen Sie eine Aufgabe zur Verteilung der Updates dieses Programms für ausgewählte Client-Geräte auf eine der folgenden Arten:
   - Um Updates auf die zur gewählten Administrationsgruppe gehörenden Client-Geräte zu verteilen, erstellen Sie eine Aufgabe für die gewählte Gruppe.
   - Um Updates auf die Client-Geräte zu verteilen, die zu unterschiedlichen oder zu keinen Administrationsgruppen gehören, erstellen Sie eine Aufgabe für eine Reihe von Geräten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie seinen Anweisungen, indem Sie wie folgt vorgehen:

   a. Im Fenster des Assistenten **Aufgabentyp** im Knoten des entsprechenden Programms wählen Sie die Aufgabe zur Verteilung der Updates.

      Die Bezeichnung der Aufgabe zur Verteilung von Updates, die im Fenster **Aufgabentyp** angezeigt wird, hängt vom Programm ab, für welches die Aufgabe erstellt wird. Für ausführliche Informationen über die Bezeichnungen der Update-Aufgaben für ausgewählte Kaspersky-Anwendungen, siehe Handbücher zu diesen Anwendungen.

   b. Im Fenster des Assistenten **Zeitplan** im Feld **Start nach Zeitplan** wählen Sie die Startvariante **Nach dem Herunterladen von Updates in die Datenverwaltung**.

   Die Aufgabe zur Verteilung von Updates wird für ausgewählte Geräte jedes Mal nach dem Herunterladen von Updates in die Datenverwaltung des Administrationsservers gestartet.

Wenn die Aufgabe zur Verteilung von Updates eines bestimmten Programms für ausgewählte Geräte bereits erstellt wurde, muss für die automatische Verteilung der Updates auf Client-Geräte im Eigenschaftenfenster im Abschnitt **Zeitplan** die Startvariante **Nach dem Herunterladen von Updates in die Datenverwaltung** im Feld **Start nach Zeitplan** ausgewählt werden.

Updates automatisch an sekundäre Administrationsserver verteilen

Damit Updates für das ausgewählte Programm sofort nach dem Update-Download in die Datenverwaltung des primären Administrationsservers automatisch an die sekundären Administrationsserver verteilt werden:

1. Wählen Sie in der Konsolenstruktur im Knoten des primären Administrationsservers den Ordner **Aufgaben** aus.
2. Wählen Sie in der Aufgabenliste des Arbeitsbereichs die Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers aus.

3. Öffnen Sie den Abschnitt **Einstellungen** im Eigenschaftenfenster der ausgewählten Aufgabe auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie auf den Link **Einstellungen anpassen** im Informationsfeld der ausgewählten Datei.

4. Öffnen Sie im Abschnitt **Einstellungen** im Eigenschaftenfenster der Aufgabe das Fenster **Sonstige Einstellungen**, indem Sie auf den Link **Anpassen** im Unterabschnitt Sonstige Einstellungen klicken.

5. Aktivieren Sie im folgenden Fenster **Sonstige Einstellungen** das Kontrollkästchen **Update sekundärer Administrationsserver erzwingen**.

6. Aktivieren Sie im Eigenschaftenfenster der Aufgabe "Update-Download durch Administrationsserver" auf der Registerkarte **Einstellungen** das Kontrollkästchen **Update sekundärer Administrationsserver erzwingen**.

Nach Abschluss des Update-Downloads durch den primären Administrationsserver werden auf den sekundären Administrationsserver die Aufgaben zum Update-Download automatisch gestartet. Dies geschieht unabhängig von dem Zeitplan, der in den Aufgabeneinstellungen angegeben ist.

Der primäre Administrationsserver führt Updates der Antiviren-Datenbanken entsprechend den auf den sekundären Administrationsservern installierten Anwendungen durch. Die Installation zusätzlicher Plug-ins und die Erstellung von Installationspaketen auf dem primären Administrationsserver ist nicht erforderlich.

Verteilungspunkte automatisch zuweisen

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. Kaspersky Security Center wählt dann selbst aus, welche Geräte zu Verteilungspunkten zugewiesen werden.

Um Verteilungspunkte automatisch zuzuweisen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des Administrationsservers aus, für den Sie Verteilungspunkte automatisch zuweisen möchten.

3. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.

4. Wählen Sie im Fenster "Eigenschaften des Administrationsservers" im Bereich **Abschnitte** die Option **Verteilungspunkte** aus.

5. Wählen Sie im rechten Teil des Fensters die Option **Verteilungspunkte automatisch zuweisen**.

   Wenn die automatische Gerätezuweisung für Verteilungspunkte aktiviert ist, können die Einstellungen der Verteilungspunkte nicht manuell angepasst werden und die Liste der Verteilungspunkte kann nicht verändert werden.

6. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin beginnt der Administrationsserver damit, Verteilungspunkte automatisch zu bestimmen und ihre Einstellungen zu konfigurieren.

Gerät manuell zum Verteilungspunkt bestimmen

In Kaspersky Security Center haben Sie die Möglichkeit, Geräte zu Verteilungspunkten zu bestimmen.

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. In diesem Fall wählt Kaspersky Security Center die Geräte, die zu Verteilungspunkten bestimmt werden, selbständig aus. Wenn Sie jedoch aus bestimmten Gründen auf die automatische Bestimmung der Verteilungspunkte verzichten möchten (beispielsweise wenn Sie speziell ausgewählte Server verwenden wollen), können Sie die Verteilungspunkte manuell bestimmen, nachdem Sie deren Anzahl und Konfiguration berechnet haben.

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Um ein Gerät manuell zum Verteilungspunkt zu bestimmen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Verteilungspunkte** aus und klicken Sie auf die Schaltfläche **Hinzufügen**. Die Schaltfläche ist verfügbar, wenn **Verteilungspunkte manuell zuweisen** ausgewählt wurde.

   Das Fenster **Verteilungspunkt hinzufügen** wird geöffnet.
4. Gehen Sie im Fenster **Verteilungspunkt hinzufügen** wie folgt vor:

   a. Wählen Sie das Gerät aus, das die Rolle des Verteilungspunkts übernehmen soll (wählen Sie dieses in der Administrationsgruppe aus oder geben Sie die IP-Adresse des Geräts an). Berücksichtigen Sie bei der Auswahl des Geräts die Besonderheiten des Verteilungspunkts und die Anforderungen an das Gerät, das die Rolle des Verteilungspunkts übernehmen soll.

   b. Geben Sie eine Reihe von Geräten an, an die der Verteilungspunkt Updates verteilen soll. Sie können eine Administrationsgruppe oder eine Beschreibung des Netzwerkspeicherorts angeben.
5. Klicken Sie auf die Schaltfläche **OK**.

   Der hinzugefügte Verteilungspunkt wird in der Liste der Verteilungspunkte im Abschnitt **Verteilungspunkte** angezeigt.
6. Wählen Sie den hinzugefügten Verteilungspunkt in der Liste aus und öffnen Sie mithilfe der Schaltfläche **Eigenschaften** das entsprechende Eigenschaftenfenster.
7. Passen Sie im Eigenschaftenfenster die Einstellungen des Verteilungspunkts an:

   - Der Abschnitt **Allgemein** enthält die Einstellungen für die Interaktion des Verteilungspunkts mit den Client-Geräten.

     - **SSL-Port**

       Nummer des SSL-Ports, über den die geschützte Verbindung des Client-Geräts mit dem Verteilungspunkt über das SSL-Protokoll erfolgt.

       Standardmäßig ist die Portnummer 13000 festgelegt.

- **Multicast verwenden**

  Wenn diese Option aktiviert ist, werden die Installationspakete automatisch mithilfe von IP-Multicasting an die Client-Geräte innerhalb einer Gruppe verteilt.

  IP-Multicasting erhöht die Dauer für die Installation einer Anwendung aus einem Installationspaket in eine Gruppe von Client-Geräten. Dagegen reduziert es die Installationsdauer, wenn Sie eine Anwendung auf einem einzelnen Client-Gerät installieren.

- **IP-Versand-Adresse**

  IP-Adresse, die für das Multicasting verwendet wird. Die IP-Adresse kann man im Bereich 224.0.0.0 – 239.255.255.255 festgelegt werden.

  Standardmäßig weist Kaspersky Security Center automatisch eine eindeutige IP-Multicast-Adresse im angegeben Bereich zu.

- **Port des IP-Multicast**

  Portnummer für das IP-Multicasting.

  Standardmäßig wird Port 15001 verwendet. Wenn als Verteilungspunkt ein Gerät angegeben wurde, auf dem der Administrationsserver installiert ist, wird für die Verbindung mit dem SSL-Protokoll standardmäßig Port 13001 verwendet.

- **Updates verteilen**

  Aus den folgenden Quellen werden Updates an verwaltete Geräte verteilt:

  - Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
  - Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

  Wenn Sie zur Bereitstellung von Updates Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

  Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Update-Downloads und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

- **Installationspakete verteilen**

  Aus den folgenden Quellen werden Installationspakete an verwaltete Geräte verteilt:

  - Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
  - Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

  Wenn Sie zur Bereitstellung von Installationspaketen Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

  Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Downloads von Installationspaketen und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

- **Diesen Verteilungspunkt als Push-Server verwenden**

  In Kaspersky Security Center kann ein Verteilungspunkt als Push-Server für Geräte fungieren, die über das mobile Protokoll verwaltet werden. Ein Push-Server muss beispielsweise aktiviert sein, wenn Sie die erzwungene Synchronisierung von KasperskyOS-Geräten mit dem Administrationsserver verwenden möchten. Ein Push-Server besitzt denselben Umfang verwalteter Geräte wie der Verteilungspunkt, auf dem der Push-Server aktiviert ist. Wenn Sie mehrere Verteilungspunkte derselben Administrationsgruppe zugewiesen haben, können Sie den Push-Server auf jedem der Verteilungspunkte aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

  Wenn Sie Geräte verwalten, auf denen KasperskyOS installiert ist, oder wenn Sie dies planen, müssen Sie einen Verteilungspunkt als Push-Server verwenden. Sie können einen Verteilungspunkt auch als Push-Server verwenden, wenn Sie Push-Nachrichten an Client-Geräte senden möchten.

- **Port des Push-Servers**

  Das ist der Port des Verteilungspunkts, den die Client-Geräte für die Verbindung verwenden. Standardmäßig ist die Portnummer 13295 festgelegt.

- Geben Sie im Abschnitt **Bereich** den Bereich an, auf den der Verteilungspunkt die Updates verteilen soll (Administrationsgruppen und/oder Netzwerkspeicherort).

- Im Abschnitt **KSN Proxy** können Sie das Programm anpassen, um den Verteilungspunkt zum Weiterleiten von KSN-Anfragen von den verwalteten Geräten zu verwenden.

  - **KSN Proxy auf Seite des Verteilungspunkts aktivieren**

    Der KSN-Proxy-Service wird auf dem Gerät ausgeführt, das als Verteilungspunkt verwendet wird. Verwenden Sie diese Funktion, um Datenverkehr im Netzwerk neu zu verteilen und zu optimieren.

    Der Verteilungspunkt sendet die KSN-Statistik, die in der Erklärung zu Kaspersky Security Network aufgeführt sind, an Kaspersky.

    Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn im Fenster mit den Eigenschaften des Administrationsservers die Optionen **Administrationsserver als Proxyserver verwenden** und **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** aktiviert sind.

    Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

  - **KSN-Anfragen an Administrationsserver weiterleiten**

    Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an den Administrationsserver weiter.

    Diese Option ist standardmäßig aktiviert.

  - **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**

    Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an die KSN Cloud oder an KPSN weiter. KSN-Anfragen, die der Verteilungspunkt selbst generiert, werden ebenso direkt an KSN Cloud oder KPSN gesendet.

    Verteilungspunkte, auf denen der Administrationsagent bis einschließlich Version 11 installiert ist, können nicht direkt auf KPSN zugreifen. Um die Verteilungspunkte so anzupassen, dass KSN-Anfragen an KPSN gesendet werden, aktivieren Sie für jeden Verteilungspunkt die Option **KSN-Anfragen an den Administrationsserver weiterleiten**.

    Verteilungspunkte, auf denen der Administrationsagent ab Version 12 installiert ist, können direkt auf KPSN zugreifen.

- **Proxyserver-Einstellungen beim Verbinden mit KPSN ignorieren**

  Aktivieren Sie diese Option, wenn Sie die Proxyserver-Einstellungen in den Eigenschaften des Verteilungspunkts oder in der Richtlinie des Administrationsagenten angepasst haben, aber Ihre Netzwerkarchitektur eine direkte Verwendung von KPSN erfordert. Andernfalls können Anfragen von den verwalteten Apps KPSN nicht erreichen.

  Diese Option ist verfügbar, wenn Sie die Option **Direkt über das Internet auf KSN Cloud/KPSN zugreifen** auswählen.

- **TCP-Port**

  Die Nummer des TCP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Standardmäßig wird Portnummer 13111 verwendet.

- **UDP-Port**

  Wenn es erforderlich ist, dass sich der Administrationsagent über einen UDP-Port mit dem Administrationsserver verbindet, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine **UDP-Portnummer** an. Diese Option ist standardmäßig aktiviert. Der standardmäßige UDP-Port für die Verbindung zum Administrationsserver ist 15000.

- **HTTPS-Port**

  Wenn es erforderlich ist, dass sich die verwalteten Geräte über einen HTTPS-Port mit dem KSN-Proxyserver verbinden, aktivieren Sie die Option **HTTPS-Port verwenden** und geben Sie im Feld **HTTPS über Port** eine Nummer an. Der standardmäßige HTTPS-Port für die Verbindung zum KSN-Proxyserver ist 17111.

- Passen Sie im Abschnitt **Gerätesuche** die Einstellungen für die Abfrage der Windows-Domänen, des Active Directory oder des IP-Bereichs nach Verteilungspunkt an.

  - **Windows-Domänen**

    Sie können für Windows-Domänen die Gerätesuche erlauben und den Zeitplan für die Abfrage festlegen.

  - **Active Directory**

    Sie können für Active Directory die Netzwerkabfrage erlauben und den Zeitplan für die Abfrage festlegen.

    Wenn Sie einen Windows-Verteilungspunkt verwenden, können Sie eine der folgenden Optionen auswählen:

    - **Aktuelle Domäne des Active Directory abfragen**.
    - **Domänengesamtstruktur des Active Directory abfragen**.
    - **Angegebene Domänen des Active Directory abfragen**. Wenn Sie diese Option auswählen, fügen Sie eine oder mehrere Active Directory-Domänen zur Liste hinzu.

    Wenn Sie einen Linux-Verteilungspunkt mit installiertem Administrationsagenten Version 15 verwenden, können Sie nur Active Directory-Domänen abfragen, für die Sie die Adresse und die Anmeldeinformationen des Benutzers angeben. Die Abfrage der aktuellen Active Directory-Domäne und der Active Directory-Domänen-Gesamtstruktur ist nicht verfügbar.

  - **IP-Bereiche**

    Sie können die Gerätesuche für IPv4-Bereiche und IPv6-Netzwerke aktivieren.

Wenn Sie die Option **Abfrage des Bereichs zulassen** aktivieren, können Sie zu untersuchende Bereiche hinzufügen und den Zeitplan für sie festlegen. Sie können IP-Bereich zur Liste der untersuchten Bereiche hinzufügen.

Wenn Sie die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** aktiviert haben, fragt der Verteilungspunkt das IPv6-Netzwerk automatisch unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. In diesem Fall werden angegebene IP-Bereiche ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt. Für Verteilungspunkte mit Linux ist die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** verfügbar. Um die Zeroconf-IPv6-Abfrage verwenden zu können, müssen Sie das Tool "avahi-browse" auf dem Verteilungspunkt installieren.

- Geben Sie im Abschnitt **Erweitert** den Ordner an, den der Verteilungspunkt zum Speichern der zu verteilenden Daten verwenden soll.

  - **Standardordner verwenden**

    Bei Auswahl dieser Option wird zum Speichern der Ordner auf dem Verteilungspunkt verwendet, in dem der Administrationsagent installiert wurde.

  - **Angegebenen Ordner verwenden**

    Bei Auswahl dieser Option können Sie im unteren Feld den Pfad zum Ordner angeben. Dabei können Sie einen lokalen Ordner des Verteilungspunkts oder einen Ordner auf einem beliebigen, sich im Unternehmensnetzwerk befindlichen Remote-Gerät angeben.

    Das Benutzerkonto, unter dem der Administrationsagent auf dem Verteilungspunkt gestartet wird, muss über die Lese- und Schreibberechtigungen für den angegebenen Ordner verfügen.

Daraufhin übernehmen die ausgewählten Geräte die Rolle des Verteilungspunkts.

Nur Geräte unter der Verwaltung von Windows können ihren Netzwerkspeicherort ermitteln. Die Bestimmung des Netzwerkspeicherorts ist für Geräte unter der Verwaltung anderer Betriebssysteme nicht verfügbar.

Gerät aus der Liste der Verteilungspunkte entfernen

Um ein Gerät aus der Liste der Verteilungspunkte zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Verteilungspunkte** ein Gerät aus, das als Verteilungspunkt dient, und klicken Sie auf die Schaltfläche **Entfernen**.

Daraufhin wird das Gerät aus der Liste der Verteilungspunkte entfernt und übernimmt nicht länger die Funktion eines Verteilungspunkts.

Ein Gerät, dem automatisch die Rolle des Administrationsservers zugewiesen wurde, kann nicht aus der Liste der Verteilungspunkte gelöscht werden.

Updates über Verteilungspunkte empfangen

In Kaspersky Security Center können die Verteilungspunkte Updates vom Administrationsserver, von den Servern von Kaspersky, aus lokalen oder Netzwerkordnern abrufen.

Wenn Sie keine Update-Quelle angeben müssen, wird für eine Administrationsgruppe die Verwendung einer *Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte* empfohlen. Weitere Informationen dazu finden Sie in diesem Abschnitt Erstellen einer Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte.

Um den Update-Download für den Verteilungspunkt anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Verteilungspunkte** den Verteilungspunkt aus, über den Updates auf die Client-Geräte der Gruppe heruntergeladen werden sollen.
4. Öffnen Sie mithilfe der Schaltfläche **Eigenschaften** das Eigenschaftenfenster des Verteilungspunkts.
5. Wählen Sie im Eigenschaftenfenster des Verteilungspunkts den Abschnitt **Quellen der Updates** aus.
6. Wählen Sie die Update-Quelle für den Verteilungspunkt:
   - Damit der Verteilungspunkt die Updates vom Administrationsserver erhält, wählen Sie die Option **Vom Administrationsserver beziehen**:
     - **Diff-Dateien herunterladen**

       Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

       Diese Option ist standardmäßig aktiviert.
   - Damit der Verteilungspunkt die Updates von einer Aufgabe erhält, wählen Sie Option **Aufgabe zum erzwungenen Download von Updates verwenden**:
     - Klicken Sie auf die Schaltfläche **Auswählen**, wenn sich auf dem Gerät bereits eine solche Aufgabe befindet, und wählen Sie die Aufgabe in der entsprechenden Liste aus.
     - Klicken Sie auf die Schaltfläche **Neue Aufgabe**, um eine Aufgabe zu erstellen, wenn es auf dem Gerät noch keine solche Aufgabe gibt. Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Die Aufgabe zum Updates in die Datenverwaltung der Verteilungspunkte herunterladen ist lokal. Für jedes Gerät, das die Rolle eines Verteilungspunkts übernimmt, muss eine separate Aufgabe erstellt werden.

Daraufhin bezieht der Verteilungspunkt die Updates von der angegebenen Quelle.

Software-Updates aus der Datenverwaltung löschen

Gehen Sie folgendermaßen vor, um Programm-Updates aus der Datenverwaltung des Administrationsservers zu löschen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Software-Updates** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Software-Updates** das Update, das gelöscht werden soll.
3. Wählen Sie im Kontextmenü des Updates die Option **Update-Dateien löschen**.

Die Programm-Updates werden aus der Datenverwaltung des Administrationsservers gelöscht.

Patchinstallation für eine Kaspersky-Anwendung im Cluster-Modell

Kaspersky Security Center unterstützt nur die manuelle Installation von Patches für Kaspersky-Anwendungen im Cluster-Modell.

Um einen Patch für eine Kaspersky-Anwendungen zu installieren, gehen Sie wie folgt vor:

1. Laden Sie den Patch auf jeden Knoten des Clusters.
2. Starten Sie die Installation des Patches auf dem aktiven Knoten.
3. Warten Sie die erfolgreiche Installation des Patches ab.
4. Starten Sie den Patch auf allen untergeordneten Knoten des Clusters der Reihe nach.

   Wenn Sie den Patch aus der Befehlszeile starten, verwenden Sie den Parameter `-CLUSTER_SECONDARY_NODE`.

   Als Resultat der Ausführung dieser Aktionen wird der Patch auf jedem Knoten des Clusters installiert.
5. Führen Sie die Cluster-Dienste von Kaspersky manuell aus.

Jeder Knoten des Clusters wird in der Verwaltungskonsole als Gerät mit installiertem Administrationsagenten angezeigt.

Informationen über die installierten Patches finden Sie im Ordner **Software-Updates** oder im Bericht über die Update-Versionen der Kaspersky-Anwendungsmodule der Kaspersky-Anwendungen.

Verwalten von Programmen von Drittanbietern auf Client-Geräten

Kaspersky Security Center ermöglicht die Verwaltung von Anwendungen von Kaspersky und anderen Herstellern, die auf Client-Geräten installiert sind.

Der Administrator kann folgende Aktionen ausführen:

- Programmkategorien anhand angegebener Kriterien erstellen
- Programmkategorien mithilfe von speziell erstellten Regeln verwalten
- Programmstart auf den Geräten verwalten
- Inventarisierung durchführen und die Programm-Registry für die auf Geräten installierten Programme führen
- Schwachstellen der Programme schließen, die auf Geräten installiert wurden
- Windows-Updates und Updates anderer Softwarehersteller auf Geräten installieren
- Verwendung von Lizenzschlüsseln für lizenzierte Programmgruppen überwachen

Über Anwendungen von Drittanbietern

Kaspersky Security Center kann Ihnen dabei helfen, auf Client-Geräten installierte Drittanbieter-Programme zu aktualisieren und die Schwachstellen in Drittanbieter-Programmen zu beheben. Kaspersky Security Center kann Drittanbieter-Programme nur von der aktuell installierten Version auf die neueste Version aktualisieren.

Die Liste mit Drittanbieter-Programmen kann geändert werden und wird dynamisch aktualisiert. Sie können überprüfen, ob Sie Drittanbieter-Programme (die auf Benutzergeräten installiert sind) mit Kaspersky Security Center aktualisieren können, indem Sie die Liste der verfügbaren Updates in der MMC-basierten Verwaltungskonsole und der Kaspersky Security Center Web Console anzeigen.

Das im Folgenden beschriebene Verfahren dient ausschließlich dazu, die Liste der Drittanbieter-Programme anzuzeigen, die über Kaspersky Security Center aktualisiert werden können. Das Ausführen der Schritte ruft die erforderlichen Informationen ab, ohne eine Aufgabe zu starten.

So zeigen Sie Liste der Drittanbieter-Programme an, die Sie mit Kaspersky Security Center in der Kaspersky Security Center Web Console aktualisieren können:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
3. Geben Sie im Schritt **Einstellungen der neue Aufgabe** des Assistenten die folgenden Einstellungen an:
   a. Wählen Sie in der Dropdown-Liste **Programm** die Option **Kaspersky Security Center** aus.
   b. Wählen Sie in dem Feld **Aufgabentyp** die Option **Erforderliche Updates installieren und Schwachstellen schließen** aus.
4. Wählen Sie im Schritt **Gültigkeitsbereich der Aufgabe** die Option **Verwaltete Geräte**.

5. Klicken Sie im Schritt **Regeln für die Installation von Updates festlegen** des Assistenten auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

6. Wählen Sie im Schritt **Regeltyp auswählen** des Assistenten die Option **Regel für Updates von Drittherstellern** aus.

7. Wählen Sie im Schritt **Allgemeine Kriterien** des Assistenten die Option **Alle Updates installieren (ausgenommen abgelehnte)** und klicken Sie anschließend auf **Weiter**.

Die Liste der Drittanbieter-Programme wird angezeigt.

Um die Liste der Drittanbieter-Programme anzuzeigen, die Sie mit Kaspersky Security Center in der MMC-basierten Konsole aktualisieren können, benötigen Sie eine Lizenz für das Schwachstellen- und Patch-Management. Andernfalls ist die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** nicht verfügbar.

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Aufgaben** aus.

3. Starten Sie über den Link **Aufgabe erstellen** den Assistenten für das Erstellen einer Aufgabe. Folgen Sie den Schritten des Assistenten.

4. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten die Option **Erforderliche Updates installieren und Schwachstellen schließen**.

5. Klicken Sie im Schritt **Regeln für die Installation von Updates festlegen** des Assistenten auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

6. Wählen Sie im Schritt **Regeltyp auswählen** des Assistenten die Option **Regel für Updates von Drittherstellern** aus.

7. Wählen Sie im Schritt **Allgemeine Kriterien** des Assistenten die Option **Alle Updates installieren (ausgenommen abgelehnte)** und klicken Sie anschließend auf **Weiter**.

Die Liste der Drittanbieter-Programme wird angezeigt.

Installieren von Software-Updates von Drittanbietern

Kaspersky Security Center ermöglicht die Verwaltung von Programm-Updates für auf Client-Geräten installierte Programme und das Schließen von Schwachstellen in Programmen von Microsoft und anderen Softwareherstellern durch die Installation erforderlicher Updates.

Kaspersky Security Center führt die Suche nach Updates mit der Aufgabe zur Suche nach Updates durch und lädt die Updates in die Update-Datenverwaltung herunter. Nach Abschluss der Update-Suche stellt das Programm dem Administrator die Informationen über die verfügbaren Updates und die Schwachstellen im Programm bereit, die mit diesen Updates geschlossen werden können

Die Informationen über die verfügbaren Microsoft Windows-Updates werden vom Windows Update Center übertragen. Der Administrationsserver kann die Rolle des Windows Update-Servers übernehmen (WSUS). Um den Administrationsserver als Windows Update-Server zu verwenden, ist es erforderlich, die Synchronisierung von Updates mit dem Windows Update Center einzustellen. Sobald die Synchronisierung der Daten mit dem Windows Update Center eingerichtet wurde, stellt der Administrationsserver im angegebenen Intervall Updates für die Windows Update-Dienste auf den Geräten bereit.

Außerdem können Programm-Updates mit der Richtlinie des Administrationsagenten verwaltet werden. Dazu ist es erforderlich, eine Richtlinie für den Administrationsagenten zu erstellen und die Einstellungen für Software-Updates in den betreffenden Fenstern des Assistenten für das Erstellen einer Richtlinie anzupassen.

Der Administrator kann sich die Liste der verfügbaren Updates im Unterordner **Software-Updates** anzeigen lassen, der zum Ordner **Programmverwaltung** gehört. Dieser Ordner enthält eine Liste der durch den Administrationsserver heruntergeladenen Updates für Microsoft-Programme und Programme anderer Softwarehersteller, die auf Geräte verteilt werden können. Nachdem Durchsicht der Informationen über die verfügbaren Updates kann der Administrator die Installation von Updates auf den Geräten durchführen.

Das Update einiger Programme von Kaspersky Security Center wird mittels Deinstallation der vorherigen Programmversion und Installation der neuen Version durchgeführt.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, ein momentan geöffnetes Drittanbieter-Programm zu schließen.

Stellen Sie sicher, dass für den primären und die sekundären Administrationsserver die Option **Schwachstellen- und Patch-Management anzeigen** in folgendem Fenster aktiviert ist: **Benutzeroberfläche anpassen**. Andernfalls verarbeitet die Aufgabe zur Update-Suche nur WSUS-Updates.

Aus Sicherheitsgründen werden alle Programm-Updates von Drittanbietern, die Sie mittels der Funktion "Schwachstellen- und Patch-Management" installieren, automatisch von den Kaspersky-Technologien auf Schadsoftware untersucht. Die Technologien werden zur automatischen Untersuchung von Dateien verwendet und umfassen die Virensuche, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung sowie Machine-Learning-Methoden.

Kaspersky-Experten führen keine manuelle Analyse von Updates für Drittanbieter-Programme durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten in derartigen Updates weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen noch führen sie an ihnen zusätzliche Analysen durch, die über die im obigen Abschnitt genannten hinausgehen.

Vor der Installation von Updates auf allen Geräten können Sie eine Probeinstallation durchführen, um sich zu vergewissern, dass die installierten Updates zu keinen Störungen der Programme auf den Geräten führen.

Szenario: Aktualisieren von Software von Drittanbietern

Dieser Abschnitt enthält ein Szenario für das Update von Drittanbieter-Programmen, die auf den Client-Geräten installiert sind. Als Drittanbieter-Programme gelten Anwendungen von Microsoft und von anderen Softwareherstellern. Updates für Microsoft-Programme werden vom Dienst "Windows Update" bereitgestellt.

Erforderliche Vorrausetzungen

Der Administrationsserver muss über eine Internetverbindung verfügen, um Updates anderer Drittanbietern-Programme, die keine Software von Microsoft darstellen, installieren zu können.

Standardmäßig ist für den Administrationsserver keine Internetverbindung erforderlich, um Software-Updates von Microsoft auf den verwalteten Geräten zu installieren. Beispielsweise können die verwalteten Geräte die Software-Updates von Microsoft direkt von den Microsoft Update-Servern oder von Windows Server herunterladen, wobei Microsoft Windows Server Update Services (WSUS) im Netzwerk Ihres Unternehmens bereitgestellt werden. Der Administrationsserver muss mit dem Internet verbunden sein, wenn Sie den Administrationsserver als WSUS-Server verwenden.

Schritte

Das Update von Drittanbieter-Programmen umfasst mehrere Schritte:

1. **Suche nach erforderlichen Updates**

   Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um die für die verwalteten Geräte erforderlichen Software-Updates von Drittanbietern zu suchen. Nach Abschluss dieser Aufgabe erhält Kaspersky Security Center eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Drittanbieter-Programme, die auf den Geräten installiert sind und die Sie in den Eigenschaften der Aufgabe angegeben haben.

   Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch vom Schnellstartassistenten für den Administrationsserver erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe, oder führen Sie den Schnellstartassistenten jetzt aus.

   Anleitung:

   - Verwaltungskonsole: Schwachstellensuche in Programmen, Zeitplan erstellen für die Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"
   - Kaspersky Security Center Web Console: Aufgabe Suche nach Schwachstellen und erforderlichen Updates erstellen, Einstellungen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"

2. **Analysieren der Liste der gefundenen Updates**

   Zeigen Sie die Liste **Software-Updates** an und entscheiden Sie, welche Updates installiert werden sollen. Um detaillierte Informationen über alle Updates anzuzeigen, klicken Sie in der Liste auf den Namen des Updates. Für jedes Update in der Liste können Sie auch die Statistiken zur Update-Installation auf Client-Geräten anzeigen.

   Anleitung:

   - Verwaltungskonsole: Informationen über verfügbare Updates anzeigen
   - Kaspersky Security Center Web Console: Informationen über verfügbare Updates für Drittanbieter-Programme anzeigen

3. **Konfigurieren der Installation von Updates**

   Wenn Kaspersky Security Center die Liste der Updates für Drittanbieter-Programme erhalten hat, können Sie diese mithilfe der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* oder *Updates von Windows Update installieren* auf den Client-Geräten installieren. Erstellen Sie eine dieser Aufgaben. Sie können diese Aufgaben entweder auf der Registerkarte **Aufgaben** erstellen oder dafür die Liste **Software-Updates** verwenden.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* dient dazu, Updates für Microsoft-Programme zu installieren, einschließlich der Updates, die vom Windows-Update-Dienst angeboten werden, sowie Updates für die Software anderer Hersteller. Beachten Sie, dass diese Aufgabe nur erstellt werden kann, wenn Sie eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" haben.

Die Aufgabe *Updates von Windows Update installieren* erfordert keine Lizenz, kann aber nur für die Installation von Windows Update-Updates verwendet werden.

Zum Installieren bestimmter Programm-Updates müssen Sie den Endbenutzer-Lizenzvertrag (EULA) für die Installationssoftware akzeptieren. Wenn Sie die EULA ablehnen, wird das Software-Update nicht installiert.

Sie können eine Aufgabe zur Update-Installation nach Zeitplan starten. Stellen Sie im Aufgabenzeitplan sicher, dass die Aufgabe zur Update-Installation erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen wurde.

Anleitung:

- Verwaltungskonsole: Schwachstellen in Programmen beheben, Informationen über verfügbare Updates anzeigen
- Kaspersky Security Center Web Console: Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen, Aufgabe "Windows-Updates installieren" erstellen, Informationen über verfügbare Updates für Drittanbieter-Programme anzeigen

4 Planen der Aufgaben

Um sicherzustellen, dass die Liste der Updates immer auf dem neuesten Stand ist, planen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* so, dass sie regelmäßig automatisch ausgeführt wird. Standardmäßig ist für die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* der manuelle Start eingestellt.

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie festlegen, dass sie mit der gleichen Häufigkeit wie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* oder seltener ausgeführt wird. Beachten Sie beim Planen der Aufgabe *Updates von Windows Update installieren*, dass Sie jedes Mal die Liste der Updates definieren müssen, bevor Sie diese Aufgabe starten.

Stellen Sie beim Planen der Aufgaben sicher, dass die Aufgabe zum Installieren der Updates erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen ist.

5 Genehmigen und Ablehnen von Programm-Updates (optional)

Falls Sie die Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellt haben, können Sie in den Aufgabeneigenschaften Regeln für die Update-Installation festlegen. Falls Sie die Aufgabe "Windows-Updates installieren" erstellt haben, überspringen Sie diesen Schritt.

Sie können für jede Regel die zu installierenden Updates abhängig vom Update-Status definieren: *Nicht definiert*, *Genehmigt* oder *Abgelehnt*. Sie können beispielsweise eine spezielle Aufgabe für Server erstellen und für diese Aufgabe festlegen, dass nur Windows-Updates mit dem Status *Genehmigt* installiert werden dürfen. Anschließend setzen Sie für jene Updates, die Sie installieren möchten, manuell den Status *Genehmigt*. In diesem Fall werden Windows-Updates, die den Status *Nicht definiert* oder *Abgelehnt* haben, auf den in der Aufgabe angegebenen Servern nicht installiert.

Bei einer geringen Menge an Updates ist das Verwenden des Status *Genehmigt* für die Verwaltung der Installation der Updates ist effizient. Für die Verwaltung mehrerer Updates können Sie die Regeln verwenden, die Sie in der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* konfigurieren können. Es wird empfohlen, den Status *Genehmigt* nur für die Updates zu setzen, die nicht den in den Regeln konfigurierten Kriterien entsprechen. Wenn Sie große Mengen an Updates manuell genehmigen, verringert sich die Leistungsfähigkeit des Administrationsservers, was zu einer Überlastung des Servers führen kann.

Standardmäßig besitzen heruntergeladene Software-Updates den Status *Nicht definiert*. Sie können den Status in der Liste **Software-Updates** auf *Genehmigt* oder *Abgelehnt* ändern (**Vorgänge** → **Patch-Management** → **Software-Updates**).

Anleitung:

- Verwaltungskonsole: Genehmigen und Ablehnen von Software-Updates
- Kaspersky Security Center Web Console: Genehmigen und Ablehnen der Updates von Drittanbieter-Programmen

6. **Administrationsserver anpassen, damit er als Server für Windows Server Update Services (WSUS) funktioniert (optional)**

   Windows-Updates werden standardmäßig von den Microsoft-Servern auf die verwalteten Geräte heruntergeladen. Sie können diese Einstellung ändern, um den Administrationsserver als WSUS-Server zu verwenden. In diesem Fall synchronisiert der Administrationsserver die Update-Daten in festgelegten Zeitabständen mit Windows Update und stellt die Updates für Windows Update im zentralisierten Modus auf den Netzwerkgeräten bereit.

   Um den Administrationsserver als WSUS-Server zu verwenden, erstellen Sie die Aufgabe "Windows-Updates synchronisieren" und aktivieren Sie das Kontrollkästchen **Administrationsserver als WSUS-Server verwenden** in der Richtlinie des Administrationsagenten.

   Anleitung:

   - Verwaltungskonsole: Windows-Updates mit dem Administrationsserver synchronisieren, Windows-Updates in der Richtlinie des Administrationsagenten anpassen
   - Kaspersky Security Center Web Console: Erstellen der Aufgabe "Windows-Updates synchronisieren"

7. **Ausführen einer Aufgabe zum Installieren von Updates**

   Starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Updates von Windows Update installieren*. Wenn Sie diese Aufgaben starten, werden die Updates heruntergeladen und auf den verwalteten Geräten installiert. Stellen Sie nach Abschluss der Aufgabe sicher, dass sie in der Liste den Status *Erfolgreich abgeschlossen* hat.

8. **Erstellen des Berichts über die Installationsergebnisse der Updates für Drittanbieter-Programme (optional)**

   Um eine detaillierte Statistik über die Update-Installation anzuzeigen, erstellen Sie den **Bericht über die Installationsergebnisse der Updates von Drittanbieterprogrammen**.

   Anleitung:

   - Verwaltungskonsole: Bericht erstellen und anzeigen
   - Kaspersky Security Center Web Console: Erzeugen und Anzeigen von Berichten

Ergebnisse

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt und angepasst haben, werden die Updates automatisch auf den verwalteten Geräten installiert. Wenn neue Updates in die Datenverwaltung des Administrationsservers heruntergeladen wurden, prüft Kaspersky Security Center, ob die Updates den Kriterien aus den Update-Regeln entsprechen. Alle neuen Updates, welche die Kriterien erfüllen, werden beim nächsten Aufgabenstart automatisch installiert.

Wenn Sie die Aufgabe *Updates von Windows Update installieren* erstellt haben, werden nur die in den Aufgabeneigenschaften *Updates von Windows Update installieren* angegeben Updates installiert. Wenn Sie in Zukunft neue Updates installieren möchten, die in die Datenverwaltung des Administrationsservers heruntergeladen wurden, müssen Sie diese in der Liste der Updates in der vorhandenen Aufgabe hinzufügen oder eine neue Aufgabe des Typs *Updates von Windows Update installieren* erstellen.

Informationen zu verfügbaren Updates für Anwendungen von Drittanbietern anzeigen

Um eine Liste der verfügbaren Updates für die auf den Client-Geräten installierten Drittanbieter-Programme anzuzeigen, gehen Sie wie folgt vor:

Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Software-Updates** aus.

Im Arbeitsbereich des Ordners können Sie sich die Liste der vorhandenen Updates für die auf den Geräten installierten Programme anzeigen lassen.

So zeigen Sie sich die Eigenschaften eines Updates an:

Klicken Sie mit der rechten Maustaste auf das erforderliche Update im Arbeitsbereich des Ordners **Software-Updates** und wählen Sie den Punkt **Eigenschaften** aus.

Im Eigenschaftenfenster des Updates werden folgende Informationen angezeigt:

- Im Abschnitt **Allgemein** können Sie den **Status der Update-Genehmigung** anzeigen:
  - **Nicht definiert** – Das Update ist in der Liste der Updates verfügbar, aber nicht zur Installation freigegeben.
  - **Genehmigt** – Das Update ist in der Liste der Updates verfügbar und zur Installation freigegeben.
  - **Abgelehnt** – Die Installation des Updates wird abgelehnt.
- Im Abschnitt **Attribute** können Sie die Werte des Felds **Wird automatisch installiert** anzeigen:
  - Der Wert **Automatisch** wird angezeigt, wenn die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* Updates für das Programm installieren kann. Das Programm installiert neue Updates automatisch mithilfe von Webadressen, die vom Hersteller des Drittanbieter-Programms zur Verfügung gestellte werden.
  - Der Wert **Manuell** wird angezeigt, wenn Kaspersky Security Center die Updates für das Programm nicht automatisch installieren kann. Sie können Updates manuell installieren.

  Das Feld **Wird automatisch installiert** wird für Updates von Windows-Programmen nicht angezeigt.
- Liste der Client-Geräte, für die das Update anwendbar ist
- Liste der systemweiten Komponenten (Voraussetzungen), die vor der Installation von Updates installiert werden müssen (falls vorhanden).
- Schwachstellen in Programmen, die durch dieses Update geschlossen werden

Genehmigen und Ablehnen von Software-Updates

Die Einstellungen einer Aufgabe zur Update-Installation erfordern eventuell die Genehmigung der zu installierenden Updates. Sie können Updates, die installiert werden müssen, genehmigen und Updates, die nicht installiert werden dürfen, ablehnen.

Beispielsweise können Sie zuerst die Installation von Updates in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb von Geräten nicht stören, und erst dann die Installation dieser Updates auf Client-Geräten erlauben.

Bei einer geringen Menge an Drittanbieter-Updates ist das Verwenden des Status *Genehmigt* für die Verwaltung der Installation der Updates ist effizient. Für die Verwaltung mehrerer Drittanbieter-Updates können Sie die Regeln verwenden, die Sie in der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* konfigurieren können. Es wird empfohlen, den Status *Genehmigt* nur für die Updates zu setzen, die nicht den in den Regeln konfigurierten Kriterien entsprechen. Wenn Sie große Mengen an Updates manuell genehmigen, verringert sich die Leistungsfähigkeit des Administrationsservers, was zu einer Überlastung des Servers führen kann.

Um ein oder mehrere Updates zu genehmigen oder abzulehnen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Erweitert** → **Programmverwaltung** → **Software-Updates** aus.
2. Klicken Sie im Arbeitsbereich des Ordners **Software-Updates** auf die Schaltfläche **Aktualisieren** in der rechten oberen Ecke. Daraufhin wird eine Liste von Updates angezeigt.
3. Wählen Sie die Updates aus, die Sie genehmigen oder ablehnen möchten.

   Das Informationsfeld für die ausgewählten Objekte wird auf der rechten Seite des Arbeitsbereichs angezeigt.
4. Wählen Sie in der Dropdown-Liste **Status der Update-Genehmigung** die Option **Genehmigt** aus, um die ausgewählten Updates zu genehmigen, bzw. **Abgelehnt**, um die ausgewählten Updates abzulehnen.

   Als Standard gilt der Wert **Nicht definiert**.

Die Updates, für die Sie den Status **Genehmigt** auswählen, werden in eine Warteschlange für die Installation verschoben.

Die Updates, für die Sie den Status **Abgelehnt** auswählen, werden von allen Geräten, auf denen Sie bisher installiert waren, (falls möglich) deinstalliert. Ferner werden sie in Zukunft nicht auf anderen Geräten installiert.

Einige Updates für die Kaspersky-Anwendungen können nicht deinstalliert werden. Wenn Sie für diese den Status **Abgelehnt** festlegen, wird Kaspersky Security Center diese Updates nicht von den Geräten deinstallieren, auf denen sie zuvor installiert waren. Diese Updates werden jedoch in Zukunft niemals auf anderen Geräten installiert. Wenn ein Update für Kaspersky-Anwendungen nicht deinstalliert werden kann, wird diese Eigenschaft in im Update-Eigenschaftenfenster angezeigt: Wählen Sie im Bereich **Abschnitte** den Punkt **Allgemein** und die Eigenschaft wird im Arbeitsbereich unter **Installationsanforderungen** angezeigt. Wenn Sie Updates für Drittanbieter-Programme den Status **Abgelehnt** zuweisen, werden die Updates nicht auf jenen Geräten installiert, auf denen sie vorgesehen waren, aber noch nicht installiert wurden. Auf den Geräten, auf denen die Updates bereits installiert wurden, bleiben diese auch weiterhin. Wenn Sie diese löschen müssen, können Sie dies manuell lokal vornehmen.

Windows-Updates mit dem Administrationsserver synchronisieren

Wenn Sie **Administrationsserver als WSUS-Server verwenden** im Fenster **Einstellungen für die Verwaltung von Updates** des Schnellstartassistenten ausgewählt haben, wird die Aufgabe zur Synchronisierung von Windows-Updates automatisch erstellt. Sie können die Aufgabe im Ordner **Aufgaben** starten. Die Funktion zum Aktualisieren der Software von Microsoft ist erst nach einem erfolgreichen Abschluss der Aufgabe **Windows-Updates synchronisieren** verfügbar.

Die Updates für Software von Microsoft können größer als 10 GB sein. Stellen Sie sicher, dass die Administrationsserver-Datenbank solche Datenmengen aufnehmen kann. Andernfalls schlägt die Aufgabe **Windows-Updates synchronisieren** fehl. Die Microsoft SQL Express-Datenbank wird für die Aufgabe **Windows-Updates synchronisieren** nicht unterstützt.

Die Aufgabe **Windows-Updates synchronisieren** lädt nur Metadaten von den Microsoft-Servern herunter. Wenn im Netzwerk kein WSUS-Server verwendet wird, lädt jedes Client-Gerät die Microsoft-Updates selbständig von externen Servern herunter.

Gehen Sie wie folgt vor, um die Aufgabe zur Synchronisierung von Windows-Updates mit dem Administrationsserver anzulegen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Software-Updates** aus.

2. Klicken Sie auf die Schaltfläche **Weitere Aktionen** und wählen Sie **Synchronisierung von Windows-Updates anpassen** in der Dropdown-Liste.

   Die vom Assistenten erstellte Aufgabe **Windows-Updates synchronisieren** wird im Ordner **Aufgaben** angezeigt.

   Assistent für das Erstellen einer Aufgabe zum Abrufen von Daten vom Windows-Updatecenter. Folgen Sie den Anweisungen des Assistenten.

Sie können eine Aufgabe zur Synchronisierung von Windows-Updates auch mit dem Link **Aufgabe erstellen** im Ordner **Aufgaben** anlegen.

Microsoft entfernt von den Servern des Unternehmens regelmäßig veraltete Updates, so dass die Zahl der aktuellen Updates zwischen 200.000 und 300.000 liegt. Um den Speicherplatzverbrauch und die Datenbankgröße zu reduzieren, löscht Kaspersky Security Center die veralteten Updates, die nicht mehr auf den Microsoft-Update-Servern vorhanden sind.

Während der Ausführung der Aufgabe **Windows-Updates synchronisieren**, erhält das Programm eine Liste der aktuellen Updates vom Update-Server von Microsoft. Danach erstellt Kaspersky Security Center eine Liste der veralteten Updates. Beim folgenden Start der Aufgabe **Suche nach Schwachstellen und erforderlichen Updates** kennzeichnet Kaspersky Security Center die veralteten Updates und bestimmt den Zeitpunkt der Entfernung. Beim folgenden Start der Aufgabe **Windows-Updates synchronisieren** werden die Updates gelöscht, die vor 30 Tagen zum Entfernen gekennzeichnet wurden. Kaspersky Security Center führt ferner eine zusätzliche Untersuchung für die Entfernung von veralteten Erneuerungen durch, die vor mehr als 180 Tagen gekennzeichnet wurden.

Nach Abschluss der Aufgabe **Windows-Updates synchronisieren** und Entfernung der veralteten Updates können die Hash-Codes der Dateien der entfernten Updates sowie die ihnen entsprechenden Dateien in der Datenbank im Ordner %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles bleiben, falls sie zuvor heruntergeladen wurden. Mithilfe der Aufgabe **Wartung des Administrationsservers** können Sie diese veralteten Einträge aus der Datenbank und den entsprechenden Dateien entfernen.

Schritt 1. Festlegen, ob der Datenverkehr reduziert werden soll

Wenn Kaspersky Security Center die Updates mit den Servern von Microsoft Windows Update Servers synchronisiert, werden Informationen über alle Dateien in der Administrationsserver-Datenbank gespeichert. Ferner werden alle Dateien, die für das Update notwendig sind, bei der Interaktion mit dem Windows Update-Agenten auf das Laufwerk heruntergeladen. Insbesondere speichert Kaspersky Security Center Informationen über die Updatedateien für die Expressinstallation in der Datenbank und lädt sie bei Bedarf. Wenn Sie Updatedateien für Expressinstallation herunterladen wird der freie Speicherplatz auf dem Laufwerk verringert.

Um eine Verringerung des Speicherplatzes zu verhindern und den Datenverkehr zu verringern, können Sie die Option **Dateien für Expressinstallation herunterladen** deaktivieren.

Wenn die Option aktiviert ist, werden während der Aufgabenausführung die Express-Updatedateien heruntergeladen. Diese Variante ist standardmäßig nicht ausgewählt.

Schritt 2. Anwendungen

In diesem Abschnitt können Sie Programme auswählen, für die Updates heruntergeladen werden sollen.

Wenn das Kontrollkästchen **Alle Programme** aktiviert ist, werden die Updates für alle vorhandenen Programme, sowie für jene Programme heruntergeladen, die möglicherweise in Zukunft vorhanden sein könnten.

Das Kontrollkästchen **Alle Programme** ist standardmäßig aktiviert.

Schritt 3. Update-Kategorien

In diesem Abschnitt können Sie Kategorien von Updates auswählen, die auf den Administrationsserver heruntergeladen werden sollen.

Wenn das Kontrollkästchen **Alle Kategorien** aktiviert ist, werden die Updates für alle vorhandenen Update-Kategorien, sowie für jene Kategorien heruntergeladen, die möglicherweise in Zukunft vorhanden sein könnten.

Das Kontrollkästchen **Alle Kategorien** ist standardmäßig aktiviert.

Schritt 4. Update-Sprachen

In diesem Fenster können Sie Sprachen für Updates auswählen, die auf den Administrationsserver heruntergeladen werden sollen. Wählen Sie eine der folgenden Varianten für den Download der Update-Sprachen aus:

- **Alle Sprachen (einschließlich neuer) herunterladen**

  Wurde diese Option ausgewählt, werden alle verfügbaren Sprachversionen der Updates auf den Administrationsserver heruntergeladen. Diese Variante ist standardmäßig ausgewählt.

- **Ausgewählte Sprachen herunterladen**

  Wurde diese Option ausgewählt, können Sie in der Liste Sprachen zur Lokalisierung von Updates auswählen, die auf den Administrationsserver heruntergeladen werden sollen.

Schritt 5. Auswählen des Kontos für Aufgabenausführung

Im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** können Sie festlegen, unter welchem Benutzerkonto die Aufgabe gestartet wird. Wählen Sie eine der folgenden Varianten aus:

- **Standardbenutzerkonto**

  Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

  Diese Variante ist standardmäßig ausgewählt.

- **Benutzerkonto festlegen**

  Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

  - **Benutzerkonto**

    Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

  - **Kennwort**

    Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

Schritt 6. Konfigurieren des Zeitplans für den Aufgabenstart

Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

- **Start nach Zeitplan**

  Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

  - **Alle n Stunden**

    Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

    Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

  - **Alle n Tage**

    Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

    Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

  - **Alle n Wochen**

    Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

    Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

- **Alle n Minuten**

  Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

  Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Einmal**

  Die Aufgabe wird einmal zum angegebenen Datum und zur angegebenen Uhrzeit ausgeführt (standardmäßig entspricht dies dem Tag, an dem die Aufgabe erstellt wurde).

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

Schritt 7. Festlegen des Aufgabennamens

Geben Sie im Fenster **Aufgabenname festlegen** den Namen der Regel an, die Sie erstellen. Ein Aufgabenname darf nicht mehr als 100 Zeichen und keine Sonderzeichen (wie `"*<>?\:|`) enthalten. Der Standardwert lautet *Windows-Updates synchronisieren*.

Schritt 8. Abschließen der Aufgabenerstellung

Klicken Sie im Fenster **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistent abzuschließen.

Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Die erstellte Aufgabe "Windows-Updates synchronisieren" wird in der Aufgabenliste im Ordner **Aufgaben** des Konsolenbaums angezeigt.

Manuelle Installation von Updates auf Geräte

Wenn Sie im Schnellstartassistenten auf der Seite **Einstellungen für die Verwaltung von Updates** die Option **Erforderliche Updates suchen und installieren** ausgewählt haben, wird die Aufgabe *Installation erforderlicher Updates und Schließen von Schwachstellen* automatisch erstellt. Sie können die Aufgabe im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** beenden oder starten.

Wenn Sie im Schnellstartassistenten die Variante **Erforderliche Updates suchen** ausgewählt haben, können Sie Programm-Updates mit der Aufgabe *Installation erforderlicher Updates und Schließen von Schwachstellen* auf den Client-Geräten installieren.

Sie können eine der folgenden Aktionen durchführen:

- Eine Aufgabe zum Installieren von Updates erstellen.
- Eine Regel zum Installieren eines Updates zu einer bestehenden Aufgabe zur Installation von Updates hinzufügen.
- In den Einstellungen einer bestehenden Aufgabe zur Installation von Updates eine Testinstallation für Updates anpassen.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, ein momentan geöffnetes Drittanbieter-Programm zu schließen.

Installation von Updates mittels Erstellen einer Installationsaufgabe

Sie können eine der folgenden Aktionen durchführen:

- Eine Aufgabe zum Installieren von bestimmten Updates erstellen.
- Ein Update auswählen und eine Aufgabe für dessen sowie für die Installation ähnlicher Updates erstellen.

Um bestimmte Updates zu installieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Software-Updates** aus.
2. Wählen Sie im Arbeitsbereich die Updates aus, die Sie installieren möchten.
3. Führen Sie eine beliebige der folgenden Aktionen aus:
   - Rechtsklicken Sie auf eines der ausgewählten Updates in der Liste und wählen Sie dann **Update installieren** → **Neue Aufgabe** aus.
   - Klicken Sie auf den Link **Update installieren (Aufgabe erstellen)** im Informationsfeld der ausgewählten Updates.
4. Treffen Sie in der angezeigten Eingabeaufforderung Ihre Wahl in Bezug auf die Installation aller vorherigen Anwendungs-Updates. Klicken Sie auf **Ja**, wenn Sie mit der inkrementellen Installation nachfolgender Programmversionen einverstanden sind, falls das für die Installation der ausgewählten Updates erforderlich ist. Klicken Sie auf **Nein**, wenn Sie Anwendungen auf eine geradlinige Weise aktualisieren möchten, ohne nachfolgende Versionen zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

   Daraufhin wird der Assistent für die Erstellung einer Aufgabe Programm-Updates installieren und Schwachstellen schließen gestartet. Folgen Sie den Schritten des Assistenten.

5. Wählen Sie auf der Seite **Methode zum Neustart des Betriebssystems** des Assistenten die Aktion aus, die ausgeführt werden soll, wenn das Betriebssystem auf dem Client-Gerät nach dem Vorgang neu gestartet werden muss:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

   - **Gerät neu starten**

     Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

   - **Benutzer fragen**

     Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

     Diese Option ist standardmäßig ausgewählt.

     - **Aufforderung regelmäßig wiederholen alle (Min.)**

       Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

       Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

       Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

     - **Neustart nach (Min.)**

       Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

       Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

   - **Beenden von Programmen in blockierten Sitzungen erzwingen**

     Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

     Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

     Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

     Diese Option ist standardmäßig deaktiviert.

6. Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **Start nach Zeitplan**

     Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

     - **Alle n Stunden**

       Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

       Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

     - **Alle n Tage**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

       Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

     - **Alle n Wochen**

       Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

       Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

     - **Alle n Minuten**

       Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

       Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

     - **Täglich (Sommerzeit wird nicht unterstützt)**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

       Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

       Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

     - **Wöchentlich**

       Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

     - **Nach Wochentagen**

       Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

       Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

     - **Monatlich**

       Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

- Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
- Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

  Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
- Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

7. Geben Sie auf der Seite **Aufgabenname festlegen** des Assistenten den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

8. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

   Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nach Abschluss des Assistenten wird **Erforderliche Updates installieren und Schwachstellen schließen** im Ordner **Aufgaben** angezeigt.

In den Einstellungen der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* können Sie die automatische Installation systemweiter Komponenten (Voraussetzungen) zulassen, die vor der Installation von Updates installiert werden müssen. In diesem Fall werden vor der Update-Installation alle erforderlichen systemweiten Komponenten installiert. Diese Komponenten sind in den Update-Eigenschaften aufgelistet.

In den Einstellungen der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* können Sie die Installation von Updates zulassen, bei deren Installation eine neue Programmversion installiert wird.

Wenn in den Einstellungen der Aufgabe Regeln für die Installation von Drittanbieter-Updates konfiguriert sind, lädt der Administrationsserver erforderliche Updates von der Website des Herstellers herunter. Die Updates werden in der Datenverwaltung des Administrationsservers gespeichert und auf Geräte, auf denen sie anzuwenden sind, verteilt und installiert.

Wenn in den Einstellungen der Aufgabe Regeln für die Installation von Microsoft-Updates konfiguriert sind und der Administrationsserver als WSUS-Server verwendet wird, lädt der Administrationsserver die notwendigen Updates in die Datenverwaltung und verteilt sie auf die verwalteten Geräte. Wenn im Netzwerk kein WSUS-Server verwendet wird, lädt jedes Client-Gerät die Microsoft-Updates selbständig von externen Servern herunter.

Um ein bestimmtes Update und ähnliche zu installieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Software-Updates** aus.

2. Wählen Sie im Arbeitsbereich das Update aus, das Sie installieren möchten.

3. Klicken Sie auf die Schaltfläche **Assistent zur Installation von Updates starten**.

   Der Assistent zur Installation von Updates wird gestartet.

   > Die Funktionen des Assistenten zur Installation von Updates sind nur verfügbar, wenn eine Lizenz für Schwachstellen- und Patch-Management vorhanden ist.

   Folgen Sie den Schritten des Assistenten.

4. Geben Sie auf der Seite **Vorhandene Aufgaben zur Installation von Updates suchen** die folgenden Einstellungen an:

   - **Aufgaben suchen, mit denen dieses Update installiert wird**

     Wenn diese Option aktiviert ist, sucht der Assistent zur Installation von Updates nach vorhandenen Aufgaben, mit denen das ausgewählte Update installiert wird.

     Wenn diese Option deaktiviert ist oder die Suche keine anwendbaren Aufgaben ergibt, fordert Sie der Assistent für die Installation von Updates auf, eine Regel oder Aufgabe zur Installation des Updates zu erstellen.

     Diese Option ist standardmäßig aktiviert.

   - **Installation des Updates freigeben**

     Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

     Diese Option ist standardmäßig deaktiviert.

5. Wenn Sie vorhandene Aufgaben zur Installation des Updates suchen möchten und die Suche einige Aufgaben ergibt, können Sie Eigenschaften dieser Aufgaben anzeigen oder sie manuell starten. Es sind keine weiteren Aktionen erforderlich.

   Anderenfalls klicken Sie auf die Schaltfläche **Neue Aufgabe zur Installation von Updates**.

6. Wählen Sie den Typ der Installationsregel aus, die zur neuen Aufgabe hinzugefügt werden soll, und klicken Sie dann auf die Schaltfläche **Fertigstellen**.

7. Treffen Sie in der angezeigten Eingabeaufforderung Ihre Wahl in Bezug auf die Installation aller vorherigen Anwendungs-Updates. Klicken Sie auf **Ja**, wenn Sie mit der inkrementellen Installation nachfolgender Programmversionen einverstanden sind, falls das für die Installation der ausgewählten Updates erforderlich ist. Klicken Sie auf **Nein**, wenn Sie Anwendungen auf eine geradlinige Weise aktualisieren möchten, ohne nachfolgende Versionen zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

   Daraufhin wird der Assistent für die Erstellung einer Aufgabe Programm-Updates installieren und Schwachstellen schließen gestartet. Folgen Sie den Schritten des Assistenten.

8. Wählen Sie auf der Seite **Methode zum Neustart des Betriebssystems** des Assistenten die Aktion aus, die ausgeführt werden soll, wenn das Betriebssystem auf dem Client-Gerät nach dem Vorgang neu gestartet werden muss:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

   - **Gerät neu starten**

     Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

   - **Benutzer fragen**

     Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

     Diese Option ist standardmäßig ausgewählt.

     - **Aufforderung regelmäßig wiederholen alle (Min.)**

       Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

       Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

       Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

     - **Neustart nach (Min.)**

       Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Programmen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

9. Wählen Sie auf der Seite **Geräte auswählen, denen die Aufgabe zugewiesen wird** des Assistenten eine der folgenden Optionen:

   - **Geräte auswählen, die vom Administrationsserver erkannt wurden**

     Die Aufgabe wird einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

     Sie können diese Option beispielsweise für eine Aufgabe zur Installation des Administrationsagenten auf nicht zugeordneten Geräten verwenden.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

     Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

10. Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

    - **Start nach Zeitplan**

      Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

      - **Alle n Stunden**

        Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

        Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

      - **Alle n Tage**

        Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

        Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

      - **Alle n Wochen**

        Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

        Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

      - **Alle n Minuten**

        Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

        Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

      - **Täglich (Sommerzeit wird nicht unterstützt)**

        Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

        Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

        Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

      - **Wöchentlich**

        Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

      - **Nach Wochentagen**

        Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

        Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

      - **Monatlich**

        Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell** (Standardmäßig ausgewählt)

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

- Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
- Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

  Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
- Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

11. Geben Sie auf der Seite **Aufgabenname festlegen** des Assistenten den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

12. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

    Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nach Abschluss des Assistenten wird die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** erstellt und im Ordner **Aufgaben** angezeigt.

Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Nach der Installation einer neuen Programmversion kann es in anderen Programmen zu Störungen kommen, die auf Geräten installiert sind und die von dem aktualisierten Programm abhängen.

Installation eines Updates durch Hinzufügen einer Regel zu einer vorhandenen Installationsaufgabe

Um ein Update durch Hinzufügen einer Regel zu einer vorhandenen Installationsaufgabe zu installieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Software-Updates** aus.
2. Wählen Sie im Arbeitsbereich das Update aus, das Sie installieren möchten.
3. Klicken Sie auf die Schaltfläche **Assistent zur Installation von Updates starten**.

   Der Assistent zur Installation von Updates wird gestartet.

   Die Funktionen des Assistenten zur Installation von Updates sind nur verfügbar, wenn eine Lizenz für Schwachstellen- und Patch-Management vorhanden ist.

   Folgen Sie den Schritten des Assistenten.
4. Geben Sie auf der Seite **Vorhandene Aufgaben zur Installation von Updates suchen** die folgenden Einstellungen an:

   - **Aufgaben suchen, mit denen dieses Update installiert wird**

     Wenn diese Option aktiviert ist, sucht der Assistent zur Installation von Updates nach vorhandenen Aufgaben, mit denen das ausgewählte Update installiert wird.

     Wenn diese Option deaktiviert ist oder die Suche keine anwendbaren Aufgaben ergibt, fordert Sie der Assistent für die Installation von Updates auf, eine Regel oder Aufgabe zur Installation des Updates zu erstellen.

     Diese Option ist standardmäßig aktiviert.

   - **Installation des Updates freigeben**

     Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

     Diese Option ist standardmäßig deaktiviert.
5. Wenn Sie vorhandene Aufgaben zur Installation des Updates suchen möchten und die Suche einige Aufgaben ergibt, können Sie Eigenschaften dieser Aufgaben anzeigen oder sie manuell starten. Es sind keine weiteren Aktionen erforderlich.

   Anderenfalls klicken Sie auf die Schaltfläche **Eine Update-Installationsregel hinzufügen**.

6. Wählen Sie die Aufgabe aus, zu der Sie eine Regel hinzufügen möchten, und klicken Sie dann auf die Schaltfläche **Regel hinzufügen**.

   Sie können auch Eigenschaften der vorhandenen Aufgaben anzeigen, sie manuell starten oder eine neue Aufgabe erstellen.

7. Wählen Sie den Typ der Regel aus, die zur ausgewählten Aufgabe hinzugefügt werden soll, und klicken Sie dann auf die Schaltfläche **Fertigstellen**.

8. Treffen Sie in der angezeigten Eingabeaufforderung Ihre Wahl in Bezug auf die Installation aller vorherigen Anwendungs-Updates. Klicken Sie auf **Ja**, wenn Sie mit der inkrementellen Installation nachfolgender Programmversionen einverstanden sind, falls das für die Installation der ausgewählten Updates erforderlich ist. Klicken Sie auf **Nein**, wenn Sie Anwendungen auf eine geradlinige Weise aktualisieren möchten, ohne nachfolgende Versionen zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

Eine neue Regel zur Installation des Updates wird zur vorhandenen Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** hinzugefügt.

Anpassen einer Testinstallation von Updates

Gehen Sie wie folgt vor, um die Testinstallation von Updates anzupassen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** die Aufgabe **Installation erforderlicher Updates und Schließen von Schwachstellen** aus.

2. Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Aufgabe **Installation erforderlicher Updates und Schließen von Schwachstellen** geöffnet.

3. Wählen Sie im Eigenschaftenfenster der Aufgabe im Abschnitt **Testinstallation** eine der Varianten der Testinstallation:

   - **Nicht untersuchen**. Wählen Sie diese Option aus, wenn Sie keine Testinstallation von Updates ausführen möchten.

   - **Untersuchung auf den gewählten Geräten durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf bestimmten Geräten prüfen möchten. Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie die Geräte aus, auf denen Sie die Testinstallation von Updates ausführen möchten.

   - **Untersuchung auf den Geräten in der angegebenen Gruppe durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf einer Gruppe von Geräten prüfen möchten. Geben Sie im Feld **Geben Sie eine Testgruppe an** eine Gruppe von Geräten an, auf denen eine Testinstallation ausgeführt werden soll.

   - **Untersuchung für den angegebenen Prozentsatz an Geräten durchführen**. Wählen Sie diese Option aus, wenn Sie die Untersuchung der Updates auf einem Teil der Geräte durchführen möchten. Geben Sie im Feld **Prozentsatz der Testgeräte von der gesamten Anzahl von Zielgeräten** den Prozentanteil der Geräte an, auf denen Sie die Testinstallation von Updates ausführen möchten.

4. Sobald Sie eine beliebige Option gewählt haben (mit Ausnahme von **Nicht untersuchen**), geben Sie im Feld **Zeitraum in Stunden, in dem entschieden werden soll, ob die Installation fortgesetzt wird** die Anzahl von Stunden an, die nach der Testinstallation der Updates und vor dem Beginn der Installation der Updates auf allen Geräten vergehen sollen.

Windows-Updates in der Richtlinie des Administrationsagenten anpassen

Um Windows Update in der Richtlinie des Administrationsagenten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Punkt **Verwaltete Geräte** aus.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
3. Wählen Sie eine Richtlinie für den Administrationsagenten aus.
4. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster für die Richtlinie des Administrationsagenten wird geöffnet.
5. Wählen Sie im Fensterbereich **Abschnitte** den Punkt **Software-Updates und Schwachstellen**.
6. Wählen Sie die Option **Administrationsserver als WSUS-Server verwenden**, um Windows-Updates auf den Administrationsserver herunterzuladen und sie dann auf die Client-Geräte mithilfe des Administrationsagenten zu verteilen.

   Wenn diese Option nicht aktiviert ist, werden die Windows-Updates nicht auf den Administrationsserver heruntergeladen. In diesem Fall erhalten die Client-Geräte Windows-Updates direkt von Microsoft-Servern.
7. Wählen Sie den Satz von Updates aus, welche die Benutzer auf ihren Geräten mithilfe von Windows Updates manuell installieren können

   > Wenn auf Windows 10-Geräten der Windows Update-Dienst bereits Updates für das Gerät gefunden hat, wird die neue Option, die Sie unter **Benutzern die Verwaltung von Windows-Updates erlauben** auswählen können, erst angewendet, wenn die gefundenen Updates installiert wurden.

   Wählen Sie ein Element in der Dropdown-Liste:

   - **Benutzern die Installation aller anwendbaren Windows-Updates erlauben**

     Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar sind.

     Wählen Sie diese Option aus, wenn Sie nicht in die Installation von Updates eingreifen möchten.

     > Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

   - **Benutzern nur die Installation von genehmigten Windows-Updates erlauben**

     Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar und die von Ihnen genehmigt sind.

Beispielsweise können Sie zuerst die Installation von Updates in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb von Geräten nicht stören, und erst dann die Installation dieser genehmigten Updates auf Client-Geräten erlauben.

Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

- **Benutzern die Installation von Windows-Updates nicht erlauben**

  Benutzer können Microsoft Windows-Updates nicht manuell auf Ihren Geräten installieren. Alle anwendbaren Updates werden so installiert, wie sie von Ihnen angepasst wurden.

  Wählen Sie diese Variante aus, wenn Sie die Installation von Updates zentral verwalten möchten.

  Beispielsweise können Sie den Update-Zeitplan so optimieren, dass das Netzwerk nicht überlastet wird. Sie können Updates nach Büroschluss planen, damit sie sich nicht auf die Produktivität der Benutzer auswirken.

8. Wählen Sie einen Modus für die Suche von Windows-Updates:

   - **Aktiv**

     Wenn diese Option aktiviert ist, initiiert der Administrationsserver mit Unterstützung des Administrationsagenten eine Anfrage vom Windows Update-Agent des Client-Geräts zur Update-Quelle: Windows Update Server oder WSUS. Der Administrationsagent überträgt die vom Windows Update-Agent abgerufenen Daten an den Administrationsserver.

     Die Option wird nur wirksam, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** der Aufgabe *Finden von Schwachstellen und erforderlichen Updates* ausgewählt ist.

     Diese Variante ist standardmäßig ausgewählt.

   - **Offline**

     Bei Auswahl dieser Option überträgt der Administrationsagent regelmäßig Informationen über Updates, die bei der letzten Synchronisierung des Windows Update-Agent mit der Update-Quelle abgerufen wurden, vom Windows-Update-Agenten an den Administrationsserver. Wird die Synchronisierung des Windows Update-Agenten mit der Update-Quelle nicht ausgeführt, veralten die Daten über Updates auf dem Administrationsserver.

     Wählen Sie diese Option aus, wenn Sie Updates aus dem Speicher-Cache der Update-Quelle abrufen möchten.

   - **Deaktiviert**

     Bei Auswahl dieser Option fragt der Administrationsserver keine Informationen über Updates ab.

     Wählen Sie diese Option aus, wenn Sie beispielsweise zuerst die Updates auf Ihrem lokalen Gerät testen möchten.

9. Wählen Sie die Option **Ausführbare Dateien beim Start auf Schwachstellen untersuchen**, wenn Sie ausführbare Dateien während ihrer Ausführung auf Schwachstellen untersuchen möchten.

10. Stellen Sie sicher, dass die Bearbeitung für alle Einstellungen, die Sie geändert haben, gesperrt ist. Andernfalls werden die Änderungen nicht angewendet.

11. Klicken Sie auf die Schaltfläche **Übernehmen**.

Schließen von Schwachstellen in Programmen von Drittanbietern

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center beschrieben, die sich auf das Schließen von Schwachstellen in den Programmen beziehen, die auf verwalteten Geräten installierten sind.

Szenario: Finden und Schließen von Schwachstellen in Programmen von Drittanbietern

Dieser Abschnitt enthält ein Szenario zum Auffinden und Beheben von Schwachstellen auf verwalteten Geräten unter Windows. Sie können Schwachstellen im Betriebssystem und in Drittanbieter-Programmen, einschließlich der Software von Microsoft, finden und schließen.

Erforderliche Vorrausetzungen

- Kaspersky Security Center ist in Ihrer Organisation bereitgestellt.
- Sie haben in Ihrer Organisation verwaltete Geräte, auf denen Windows ausgeführt wird.
- Damit der Administrationsserver die folgenden Aufgaben ausführen kann, ist eine Internetverbindung erforderlich:
  - Erstellen einer Liste empfohlener Korrekturen für Schwachstellen in Software von Microsoft. Die Liste wird von Kaspersky-Spezialisten erstellt und regelmäßig aktualisiert.
  - Beheben von Schwachstellen in anderer Software von Drittanbietern als Microsoft-Software.

Schritte

Das Erkennen und Schließen von Schwachstellen in Programmen erfolgt schrittweise:

1. **Scannen nach Schwachstellen in den auf den verwalteten Geräten installierten Programmen**

   Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um Schwachstellen in den auf den verwalteten Geräten installierten Programmen zu suchen. Nach Abschluss dieser Aufgabe erhält Kaspersky Security Center eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Software von Drittanbietern, die auf den Geräten installiert ist, die Sie in den Eigenschaften der Aufgabe angegeben haben.

   Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch vom Schnellstartassistent des Kaspersky Security Centers erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, starten Sie ihn jetzt oder erstellen Sie die Aufgabe manuell.

   Anleitung:

   - Verwaltungskonsole: Schwachstellensuche in Programmen, Zeitplan erstellen für die Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"
   - Kaspersky Security Center Web Console: Aufgabe Suche nach Schwachstellen und erforderlichen Updates erstellen, Einstellungen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"

2. **Analysieren der Liste der erkannten Schwachstellen in Programmen**

Zeigen Sie die Liste **Schwachstellen in Programmen** an und entscheiden Sie, welche Schwachstellen in Programmen behoben werden sollen. Um detaillierte Informationen über alle Schwachstellen anzuzeigen, klicken Sie in der Liste auf den Namen der Schwachstelle. Für jede Schwachstelle in der Liste können Sie auch eine Statistik über die Schwachstelle auf den verwalteten Geräten anzeigen.

Anleitung:

- Verwaltungskonsole: Anzeigen von Informationen zu Schwachstellen in Programmen, Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten
- Kaspersky Security Center Web Console: Informationen über Schwachstellen in Programmen anzeigen, Statistik über Schwachstellen auf verwalteten Geräten anzeigen

3 Konfigurieren von Korrekturen für Schwachstellen

Wenn Schwachstellen in Programmen erkannt werden, können Sie mithilfe der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* oder *Schwachstellen schließen* die Schwachstellen in Programmen auf den verwalteten Geräten schließen.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Drittanbieter-Programmen, einschließlich der Software von Microsoft, die auf den verwalteten Geräten installiert ist, zu aktualisieren und zu beheben. Mit dieser Aufgabe können Sie mehrere Updates installieren und mehrere Schwachstellen nach bestimmten Regeln beheben. Beachten Sie, dass diese Aufgabe nur erstellt werden kann, wenn Sie eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" haben. Um Schwachstellen in Programmen zu beheben, verwendet die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die empfohlenen Programm-Updates.

Die Aufgabe *Schwachstellen schließen* erfordert keine Lizenz-Option für die Funktion "Schwachstellen- und Patch-Management". Um die Aufgabe zu verwenden, müssen Sie manuell benutzerdefinierte Korrekturen angeben, um die Schwachstellen in Drittanbieter-Programmen zu beheben, die in den Aufgabeneinstellungen aufgeführt sind. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Microsoft-Programme und die benutzerdefinierten Korrekturen für Drittanbieter-Programme.

Sie können entweder den Assistenten für das Schließen von Schwachstellen starten, der automatisch eine dieser Aufgaben erstellt, oder Sie können eine dieser Aufgaben manuell erstellen.

Anleitung:

- Verwaltungskonsole: Auswählen von individuellen Korrekturen für Schwachstellen von Drittanbieter-Programmen, Schließen von Schwachstellen in Programmen
- Kaspersky Security Center Web Console: Auswählen von individuellen Korrekturen für Schwachstellen in Drittanbieter-Programmen, Schwachstellen in Drittanbieter-Programmen beheben, Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen

4 Planen der Aufgaben

Um sicherzustellen, dass die Liste der Schwachstellen immer auf dem neuesten Stand ist, planen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* so, dass sie regelmäßig automatisch ausgeführt wird. Die empfohlene durchschnittliche Häufigkeit ist einmal pro Woche.

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie festlegen, dass sie mit der gleichen Häufigkeit ausgeführt wird wie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* oder seltener. Beachten Sie beim planen der Aufgabe *Schwachstellen schließen*, dass Sie vor jedem Start der Aufgabe entweder Patches für Microsoft-Programme auswählen oder Patches für Drittanbieterprogramme angeben müssen.

Stellen Sie beim Planen der Aufgaben sicher, dass die Aufgabe zum Beheben von Schwachstellen erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen ist.

5 Ignorieren von Schwachstellen in Programmen (optional)

Sie können ggf. Schwachstellen in Programmen auf allen verwalteten Geräten oder nur auf den ausgewählten verwalteten Geräten ignorieren.

Anleitung:

- Verwaltungskonsole: Ignorieren von Schwachstellen in Programmen
- Kaspersky Security Center Web Console: Ignorieren von Schwachstellen in Programmen

6. **Aufgabe zum Schließen von Schwachstellen ausführen**

   Starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Schwachstelle schließen*. Stellen Sie nach Abschluss der Aufgabe sicher, dass sie in der Liste den Status *Erfolgreich abgeschlossen* hat.

7. **Bericht über die Ergebnisse des Schließens von Schwachstellen in Programmen erstellen (optional)**

   Generieren Sie den Bericht über Schwachstellen, um detaillierte Statistiken zu den behobenen Schwachstellen anzuzeigen. Der Bericht enthält Informationen über Schwachstellen in Programmen, die nicht behoben wurden. Dort können Sie sich darüber informieren, wie Sie in Ihrem Unternehmen nach Schwachstellen in Drittanbieter-Programmen, einschließlich der Software von Microsoft, suchen und solche Schwachstellen beheben können.

   Anleitung:

   - Verwaltungskonsole: Bericht erstellen und anzeigen
   - Kaspersky Security Center Web Console: Erzeugen und Anzeigen von Berichten

8. **Überprüfen der Konfiguration zum Finden und Schließen von Schwachstellen in Drittanbieter-Programmen**

   Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

   - Abrufen und Überprüfen der Liste von Schwachstellen in Programmen auf verwalteten Geräten
   - Ignorieren von Schwachstellen in Programmen, falls gewünscht
   - Konfigurieren der Aufgabe zum Schließen von Schwachstellen
   - Planen der Aufgaben zum Finden und Schließen von Schwachstellen in Programmen, sodass dass sie nacheinander gestartet werden
   - Überprüfen, ob die Aufgabe zum Schließen von Schwachstellen in Programmen ausgeführt wurde

Ergebnisse

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt und angepasst haben, werden die Schwachstellen auf den verwalteten Geräten automatisch behoben. Beim Ausführen der Aufgabe wird die Liste der verfügbaren Programm-Updates mit den Regeln abgeglichen, die in den Aufgabeneinstellungen angegeben sind. Alle Programm-Updates, welche die Kriterien der Regeln erfüllen, werden in die Datenverwaltung des Administrationsservers heruntergeladen und werden installiert, um die Schwachstellen in Programmen zu beheben.

Wenn Sie die Aufgabe *Schwachstellen schließen* erstellt haben, werden nur Schwachstellen in der Software von Microsoft geschlossen.

Über das Suchen und Schließen von Schwachstellen in Programmen

Kaspersky Security Center erkennt und behebt Schwachstellen in Programmen auf verwalteten Geräten, auf denen Microsoft Windows-Betriebssysteme ausgeführt werden. Schwachstellen werden im Betriebssystem und in Software von Drittanbietern, einschließlich Microsoft-Software, erkannt.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Software-Schwachstellen suchen

Kaspersky Security Center verwendet Merkmale aus der Datenbank mit bekannten Schwachstellen, um Schwachstellen in Programmen zu finden. Diese Datenbank wird von Kaspersky-Spezialisten erstellt. Sie enthält Informationen zu Schwachstellen, z. B. eine Beschreibung, das Datum der Erkennung und die Signifikanz der Schwachstelle. Informationen über Schwachstellen in Programmen finden Sie auf der Website von Kaspersky.

Kaspersky Security Center verwendet die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Schwachstellen in Programmen zu finden.

In bestimmten Fällen können Schwachstellen, die in einem Microsoft Windows-Betriebssystem gefunden wurden, mit einer der folgenden Methoden geschlossen werden:

- Installieren eines Updates für das Betriebssystem.
- Upgrade des Betriebssystems auf eine aktuellere Version (z. B. von Windows 10 auf Windows 11).

In diesem Szenario zeigt Kaspersky Security Center zwei Einträge für dieselbe Schwachstelle an.

Beheben von Schwachstellen in Programmen

Zum Beheben von Schwachstellen in Programmen verwendet Kaspersky Security Center die Programm-Updates der Programmhersteller. Die Metadaten des Programm-Updates werden als Ergebnis der Ausführung der folgenden Aufgabe in die Datenverwaltung des Administrationsservers heruntergeladen:

- *Download von Updates in die Datenverwaltung des Administrationsservers*. Diese Aufgabe dient dazu, Metadaten der Updates für die Software von Kaspersky und für Drittanbieter-Programme herunterzuladen. Diese Aufgabe wird automatisch vom Schnellstartassistent des Kaspersky Security Centers erstellt. Sie können die Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers manuell erstellen.
- *Windows-Updates synchronisieren*. Diese Aufgabe dient dazu, Metadaten der Updates für die Software von Microsoft herunterzuladen.

Software-Updates zur Behebung von Schwachstellen können in Form von vollständigen Programmpaketen oder Patches bereitgestellt werden. Programm-Updates, die Schwachstellen in Programmen beheben, werden als *Korrekturen* bezeichnet. *Empfohlene Korrekturen* sind solche, deren Installation von Kaspersky-Spezialisten empfohlen wird. *Individuelle Korrekturen* sind solche, die manuell für die Installation durch Benutzer ausgewählt werden. Um eine Benutzerkorrektur zu installieren, müssen Sie ein Installationspaket erstellen, das diese Korrektur enthält.

Wenn Sie über die Lizenz für Kaspersky Security Center mit der Schwachstellen- und Patch-Management-Funktion verfügen, um Schwachstellen in Programmen zu schließen, können Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* verwenden. Diese Aufgabe behebt automatisch mehrere Schwachstellen, indem empfohlene Korrekturen installiert werden. Für diese Aufgabe können Sie bestimmte Regeln manuell konfigurieren, um mehrere Schwachstellen zu beheben.

Wenn Sie nicht über die Lizenz für Kaspersky Security Center mit der Schwachstellen- und Patch-Management-Funktion verfügen, um Schwachstellen in Programmen zu schließen, können Sie die Aufgabe *Schwachstellen schließen* verwenden. Mithilfe dieser Aufgabe können Sie Schwachstellen beheben, indem empfohlene Korrekturen für die Software von Microsoft und Benutzerkorrekturen für andere Drittanbieter-Programme installiert werden.

Aus Sicherheitsgründen werden alle Programm-Updates von Drittanbietern, die Sie mittels der Funktion "Schwachstellen- und Patch-Management" installieren, automatisch von den Kaspersky-Technologien auf Schadsoftware untersucht. Die Technologien werden zur automatischen Untersuchung von Dateien verwendet und umfassen die Virensuche, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung sowie Machine-Learning-Methoden.

Kaspersky-Experten führen keine manuelle Analyse von Updates für Drittanbieter-Programme durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten in derartigen Updates weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen, noch führen sie an ihnen zusätzliche Analysen durch, die über die oben genannten hinausgehen.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie eine Drittanbieter-Anwendung aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einer Drittanbieter-Anwendung beheben. Beispielsweise kann der Benutzer aufgefordert werden, die Drittanbieter-Anwendung zu schließen, wenn es gerade geöffnet ist.

Zum Schließen bestimmter Software-Schwachstellen müssen Sie bei Aufforderung den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren. Wenn Sie die EULA ablehnen, kann die Schwachstelle nicht geschlossen werden.

Informationen über Schwachstellen in Programmen anzeigen

Um sich die Liste der Schwachstellen anzeigen zu lassen, die auf den Client-Geräten gefunden wurden,

Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

Die Seite mit der Liste von Schwachstellen in Programmen auf den verwalteten Geräten wird angezeigt.

Um Informationen über eine gewählte Schwachstelle abzufragen,

klicken Sie mit der rechten Maustaste auf die Schwachstelle und wählen Sie **Eigenschaften** aus.

Daraufhin wird das Eigenschaftenfenster der Schwachstelle geöffnet, in dem folgende Informationen angezeigt werden:

- Programm, in dem die Schwachstelle gefunden wurde
- Liste der Geräte, auf denen die Schwachstelle gefunden wurde
- Informationen zum Schließen von Schwachstellen

Um sich einen Bericht über alle gefundenen Schwachstellen anzeigen zu lassen,

Klicken Sie im Ordner **Schwachstellen in Programmen** auf den Link **Bericht über Schwachstellen anzeigen**.

Daraufhin wird ein Bericht über Schwachstellen in Programmen erstellt, die auf den Geräten vorhanden sind. Der Bericht kann im Knoten mit dem Namen des gewünschten Administrationsservers auf der Registerkarte **Berichte** angezeigt werden.

Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten

Sie können eine Statistik für jede Software-Schwachstelle auf verwalteten Geräten anzeigen. Die Statistik wird als Diagramm angezeigt. Das Diagramm enthält die Anzahl der Geräte mit den folgenden Statusvarianten:

- *Ignoriert auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie in den Eigenschaften der Schwachstelle manuell die Option zum Ignorieren der Schwachstelle festgelegt haben.
- *Geschlossen auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn die Aufgabe zum Schließen der Schwachstelle erfolgreich abgeschlossen wurde.
- *Korrektur geplant auf <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie die Aufgabe zum Schließen der Schwachstelle erstellt haben, die Aufgabe jedoch noch nicht ausgeführt wurde.
- *Patch angewendet auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie ein Programm-Update zur Behebung der Schwachstelle manuell ausgewählt haben, die Schwachstelle jedoch dadurch nicht geschlossen wurde.
- *Korrektur erforderlich auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn die Schwachstelle nur auf einigen der verwalteten Geräten geschlossen wurde und auf den anderen verwalteten Geräten noch geschlossen werden muss.

So zeigen Sie die Statistik über Schwachstelle auf einem verwalteten Gerät an:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

   Die Seite mit der Liste von Schwachstellen in Programmen auf den verwalteten Geräten wird angezeigt.

2. Wählen Sie eine Schwachstelle aus, für welche die Statistik angezeigt werden soll.

   Im Block zum Arbeiten eines ausgewählten Objektes wird ein Diagramm des Schwachstellenstatus angezeigt. Wenn Sie auf einen Status klicken, wird eine Liste der Geräte geöffnet, auf denen die Schwachstelle den ausgewählten Status hat.

Schwachstellensuche in Programmen

Wenn Sie das Programm mit dem Schnellstartassistenten konfiguriert haben, wird die Aufgabe *Untersuchung auf Schwachstellen* automatisch angelegt. Die Aufgabe kann im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** angezeigt werden.

Gehen Sie wie folgt vor, um eine Aufgabe zur Untersuchung auf Schwachstellen in den auf Client-Geräten installierten Programmen anzulegen:

1. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Programmverwaltung** aus und wählen Sie dann den Unterordner **Schwachstellen in Programmen** aus.

2. Wählen Sie im Arbeitsbereich den Punkt **Weitere Aktionen** → **Untersuchung auf Schwachstellen anpassen** aus.

   Wenn bereits eine Aufgabe zur Untersuchung auf Schwachstellen vorhanden ist, wird die Registerkarte **Aufgaben** im Ordner **Verwaltete Geräte** angezeigt und die bereits vorhandene Aufgabe markiert. Andernfalls wird der Assistent für das Erstellen einer Aufgabe zum Finden von Schwachstellen und erforderlichen Updates gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie im Fenster **Aufgabentyp auswählen** den Punkt **Suche nach Schwachstellen und erforderlichen Updates** aus.

4. Legen Sie auf der Seite **Einstellungen** des Assistenten die Aufgabeneinstellungen wie folgt fest:

   - **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

     Wenn Kaspersky Security Center nach Schwachstellen und Updates sucht, verwendet das Programm die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

     Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und Updates für Drittanbieter-Apps haben.

     Diese Option ist standardmäßig aktiviert.

     Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

     - **Mit dem Update-Server verbinden, um Daten zu aktualisieren**

       Der Windows-Update-Agent auf einem verwalteten Gerät stellt eine Verbindung zur Quelle für Microsoft-Updates her. Die folgenden Server können als Quelle für Microsoft-Updates dienen:

       - Kaspersky Security Center Administrationsserver (siehe Einstellungen der Richtlinie des Administrationsagenten)
       - Windows Server mit Microsoft Windows Server Update Services (WSUS), das in Ihrem Unternehmensnetzwerk bereitgestellt wurde
       - Microsoft-Update-Server

       Wenn diese Option aktiviert ist, stellt der Windows-Update-Agent auf einem verwalteten Gerät eine Verbindung zur Quelle für Microsoft-Updates her, um die Informationen über geeignete Microsoft-Windows-Updates zu aktualisieren.

       Wenn diese Option deaktiviert ist, verwendet der Windows-Update-Agent auf einem verwalteten Gerät die Informationen über geeignete Microsoft Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden.

       Das Herstellen einer Verbindung zur Quelle für Microsoft-Updates kann ressourcenaufwendig sein. Sie können diese Option deaktivieren, wenn Sie in einer anderen Aufgabe oder in den Eigenschaften der Administrationsagenten-Richtlinie im Abschnitt **Software-Updates und Schwachstellen** eine regelmäßige Verbindung zu dieser Update-Quelle festgelegt haben. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um eine Überlastung des Servers zu vermeiden.

Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, die in den Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Der Windows-Update-Agent auf einem verwalteten Gerät stellt nur unter den folgenden Bedingungen eine Verbindung zum Update-Server her, um Updates zu erhalten: Die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** in den Eigenschaften der Aufgabe zum *Suche nach Schwachstellen und erforderlichen Updates* ist aktiviert und die Option **Modus für die Suche nach Windows-Updates** steht in den Einstellungen der Administrationsagent-Richtlinie auf **Aktiv**.

- Wenn Sie den Administrationsagenten nicht benötigen, um während der Ausführung der Aufgabe *Untersuchung auf Schwachstellen* eine Verbindung zur Microsoft Windows-Update-Quelle herzustellen und Updates herunterzuladen, können Sie die Option **Modus für die Suche nach Windows-Updates** auf **Offline** setzen, wobei die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert bleiben muss. Auf diese Weise können Sie Ressourcen sparen und zuvor abgerufene Windows-Updates verwenden, um nach Schwachstellen zu suchen. Sie können den passiven Modus verwenden, wenn Sie das Abrufen von Microsoft Windows-Updates auf eine andere Art konfigurieren. Wenn das Abrufen von Microsoft Windows-Updates jedoch nicht auf eine andere Art konfiguriert ist, setzen Sie die Option **Modus für die Suche nach Windows-Updates** nicht auf **Offline**, da in diesem Fall keine Informationen über Updates abgerufen werden.

- Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert), wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** gesetzt ist, fragt Kaspersky Security Center keine Informationen über Updates ab.

- **Nach Schwachstellen und Updates von Drittherstellern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Security Center in der Windows-Registrierung und den unter Geben Sie Pfade für eine zusätzliche Suche nach Programmen im Dateisystem an **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für fremde Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

  Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps haben.

  Diese Option ist standardmäßig aktiviert.

- **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an**

  Die Ordner, in denen Kaspersky Security Center nach Drittanbieter-Apps sucht, für die ein Schließen von Schwachstellen und eine Update-Installation erforderlich ist. Sie können Systemvariable verwenden.

  Legen Sie die Ordner fest, in denen Programme installiert sind. Standardmäßig enthält die Liste die Systemordner, in denen die meisten Programme installiert sind.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

5. Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **Start nach Zeitplan**

     Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

     - **Alle n Stunden**

       Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

       Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

     - **Alle n Tage**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

       Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

     - **Alle n Wochen**

       Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

       Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

     - **Alle n Minuten**

       Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Nach dem Download von Updates in die Datenverwaltung**

  Die Aufgabe wird gestartet, nachdem Updates in die Datenverwaltung heruntergeladen wurden. Sie können diesen Zeitplan beispielsweise zur Suchen nach Suche nach Schwachstellen und erforderlichen Updates verwenden.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

6. Geben Sie auf der Seite **Aufgabenname festlegen** des Assistenten den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

7. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

   Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nach Abschluss des Assistenten wird die Aufgabe **Suche nach Schwachstellen und erforderlichen Updates** in der Aufgabenliste im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** angezeigt.

Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Nach der Ausführung der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* werden auf dem Administrationsserver eine Liste mit gefundenen Schwachstellen in der auf dem Gerät installierten Programme sowie die notwendigen Programm-Updates zum Schließen der gefundenen Schwachstellen angezeigt.

Wenn Sie den Fehler 0x80240033 "Windows Update Agent error 80240033 ("Lizenzvertrag konnte nicht heruntergeladen werden.")" angezeigt bekommen, können Sie dieses Problem mithilfe Windows-Registry lösen.

Der Administrationsserver zeigt die Liste der erforderlichen Programm-Updates nicht an, wenn Sie nacheinander zwei Aufgaben ausführen: zuerst die Aufgabe *Windows-Updates synchronisieren*, für welche die Option **Dateien für Express-Installation herunterladen** deaktiviert ist, und anschließend die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*. Um die Liste der erforderlichen Programm-Updates anzuzeigen, müssen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erneut ausführen.

Der Administrationsagent erhält Informationen über verfügbare Updates für Windows und andere Software von Microsoft vom Dienst Windows Update-Agent oder vom Administrationsserver, falls dieser als WSUS-Server verwendet wird. Die Informationen werden zum Zeitpunkt des Programmstarts (falls in der Richtlinie festgelegt) und beim regelmäßigen Start der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* auf den Client-Geräten übergeben.

Schließen von Schwachstellen in Programmen

Wenn Sie im Schnellstartassistenten auf der Seite **Einstellungen für die Verwaltung von Updates** die Option **Erforderliche Updates suchen und installieren** ausgewählt haben, wird die Aufgabe *Installation erforderlicher Updates und Schließen von Schwachstellen* automatisch erstellt. Die Aufgabe wird im Arbeitsbereich des Ordners **Verwaltete Geräte** auf der Registerkarte **Aufgaben** angezeigt.

Anderenfalls können Sie eine der folgenden Aktionen durchführen:

- Eine Aufgabe zum Schließen von Schwachstellen durch Installation von Updates erstellen
- Eine Regel zum Schließen einer Schwachstelle zu einer vorhandenen Aufgabe zum Schließen von Schwachstellen hinzufügen

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, ein momentan geöffnetes Drittanbieter-Programm zu schließen.

Schwachstellen durch Erstellen einer Aufgabe zum Schließen von Schwachstellen schließen

Sie können eine der folgenden Aktionen durchführen:

- Eine Aufgabe zum Schließen mehrerer Schwachstellen, die bestimmten Regeln entsprechen, erstellen
- Eine Schwachstelle auswählen und eine Aufgabe zum Schließen derselben und ähnlicher Schwachstellen erstellen

Um Schwachstelle zu schließen, die bestimmten Regeln entsprechen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver auf Geräten aus, für die Sie Schwachstellen beheben möchten.
2. Wählen Sie im Programmhauptfenster im Menü **Ansicht** den Punkt **Benutzeroberfläche anpassen**.
3. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Schwachstellen- und Patch-Management anzeigen** klicken Sie anschließend auf **OK**.
4. Klicken Sie im Fenster mit den Programm-Meldungen auf die Schaltfläche **OK**.
5. Starten Sie die Verwaltungskonsole neu, damit die Änderungen wirksam werden.
6. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
7. Wählen Sie im Arbeitsbereich die Registerkarte **Aufgaben** aus.
8. Starten Sie über den Link **Aufgabe erstellen** den Assistenten für das Erstellen einer Aufgabe. Folgen Sie den Schritten des Assistenten.

9. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten **Erforderliche Updates installieren und Schwachstellen schließen**.

   Wenn die Aufgabe nicht angezeigt wird, prüfen Sie, ob Ihr Benutzerkonto über die Berechtigungen **Lesen**, **Ändern** und **Ausführen** für den Funktionsbereich **Systemverwaltung**: **Schwachstellen- und Patch-Management** verfügt. Sie könne die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen"* ohne diese Zugriffsrechte nicht erstellen und konfigurieren.

10. Legen Sie auf der Seite **Einstellungen** des Assistenten die Aufgabeneinstellungen wie folgt fest:

    - **Regeln für die Installation von Updates festlegen**

      Diese Regeln werden für die Installation von Updates auf Client-Geräten übernommen. Wenn keine Regeln festgelegt sind, wird die Aufgabe nicht ausgeführt. Informationen über Vorgänge mit Regeln finden Sie unter Regeln zur Installation von Updates.

    - **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen**

      Ist diese Option aktiviert, so werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Andernfalls werden Updates nach einem Zeitplan installiert.

      Verwenden Sie diese Option, wenn die Installation von Updates die Geräteleistung beeinträchtigen könnte.

      Diese Option ist standardmäßig deaktiviert.

    - **Erforderliche Systemkomponenten installieren**

      Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

      Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

      Diese Option ist standardmäßig deaktiviert.

    - **Installation einer neuen Programmversion beim Update zulassen**

      Ist diese Option aktiviert, so werden Updates erlaubt, wenn sie zur Installation einer neuen Version einer Softwareanwendung führen.

      Wenn diese Option deaktiviert ist, wird die Software nicht aktualisiert. Sie können dann neue Versionen der Software manuell oder über eine andere Aufgabe installieren. Sie können diese Option beispielsweise verwenden, wenn die Infrastruktur Ihres Unternehmens nicht von einer neuen Softwareversion unterstützt wird oder wenn Sie ein Update in einer Testinfrastruktur überprüfen möchten.

      Diese Option ist standardmäßig aktiviert.

      > Aktualisieren einer Anwendung kann zu Fehlern bei abhängigen Anwendungen führen, die auf Client-Geräten installiert sind.

    - **Updates auf das Gerät herunterladen, ohne sie zu installieren**

      Wenn diese Option aktiviert ist, lädt die Anwendung Updates auf das Gerät herunter, installiert sie jedoch nicht automatisch. Sie können die heruntergeladenen Updates dann manuell installieren.

      Microsoft-Updates werden in den Windows-Systemspeicher heruntergeladen. Updates für Drittanbieter-Anwendungen (Anwendungen, die von den Software-Herstellern Kaspersky oder Microsoft stammen) werden in den Ordner heruntergeladen, der im Feld **Updates herunterladen nach** angegeben ist.

      Wenn diese Option deaktiviert ist, werden die Updates automatisch auf dem Gerät installiert.

Diese Option ist standardmäßig deaktiviert.

- **Updates herunterladen nach**

  Dieser Ordner wird verwendet, um Updates für Drittanbieter-Anwendungen (Anwendungen, die nicht von den Software-Herstellern Kaspersky oder Microsoft stammen) herunterzuladen.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

11. Wählen Sie auf der Seite **Methode zum Neustart des Betriebssystems** des Assistenten die Aktion aus, die ausgeführt werden soll, wenn das Betriebssystem auf dem Client-Gerät nach dem Vorgang neu gestartet werden muss:

    - **Gerät nicht neu starten**

      Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

    - **Gerät neu starten**

      Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

    - **Benutzer fragen**

      Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

Diese Option ist standardmäßig ausgewählt.

- **Aufforderung regelmäßig wiederholen alle (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neustart nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Programmen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

12. Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

    - **Start nach Zeitplan**

      Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

      - **Alle n Stunden**

        Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

        Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

      - **Alle n Tage**

        Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

        Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

      - **Alle n Wochen**

        Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

- **Alle n Minuten**

  Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

  Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

13. Geben Sie auf der Seite **Aufgabenname festlegen** des Assistenten den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

14. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

    Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nach Abschluss des Assistenten wird die Aufgabe **Installation erforderlicher Updates und Schließen von Schwachstellen** erstellt, die im Ordner **Aufgaben** angezeigt wird.

Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Wenn die Ergebnisse der Aufgabe den Fehler 0x80240033 "Windows Update Agent error 80240033 ("Lizenzvertrag konnte nicht heruntergeladen werden.")" enthalten, können Sie das Problem mithilfe Windows-Registry lösen.

Um eine bestimmte Schwachstelle und ähnliche zu schließen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

2. Wählen Sie die Schwachstelle aus, die Sie schließen möchten.

3. Klicken Sie auf die Schaltfläche **Assistent zum Schließen von Schwachstellen starten**.

   Der Assistent zum Schließen von Schwachstellen wird geöffnet.

   Das Funktional des Assistenten zum Schließen von Schwachstellen starten ist aktiv, wenn eine Lizenz für die Funktion Schwachstellen- und Patch-Management vorhanden ist.

   Folgen Sie den Schritten des Assistenten.

4. Legen Sie im Fenster **Bestehende Aufgaben zum Schließen von Schwachstellen suchen** die folgenden Einstellungen fest:

   - **Nur Aufgaben anzeigen, die diese Schwachstelle schließen**

     Wenn diese Option aktiviert ist, sucht der Assistent zum Schließen von Schwachstellen nach vorhandenen Aufgaben, mit denen die ausgewählte Schwachstelle geschlossen werden kann.

     Wenn diese Option deaktiviert ist oder die Suche keine anwendbaren Aufgaben ergibt, fordert Sie der Assistent zum Schließen von Schwachstellen auf, eine Regel oder Aufgabe zum Schließen der Schwachstelle zu erstellen.

     Diese Option ist standardmäßig aktiviert.

   - **Updates zum Schließen der ausgewählten Schwachstelle freigeben**

     Updates, die eine Schwachstelle schließen, werden für die Installation genehmigt. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

     Diese Option ist standardmäßig deaktiviert.

5. Wenn Sie bestehende Aufgaben zum Schließen von Schwachstellen suchen möchten und die Suche einige Aufgaben ergibt, können Sie Eigenschaften dieser Aufgaben anzeigen oder sie manuell starten. Es sind keine weiteren Aktionen erforderlich.

   Anderenfalls klicken Sie auf die Schaltfläche **Neue Aufgabe zum Schließen von Schwachstellen**.

6. Wählen Sie den Typ der Regel zum Schließen von Schwachstellen aus, die zur neuen Aufgabe hinzugefügt werden soll, und klicken Sie dann auf die Schaltfläche **Fertigstellen**.

7. Treffen Sie in der angezeigten Eingabeaufforderung Ihre Wahl in Bezug auf die Installation aller vorherigen Anwendungs-Updates. Klicken Sie auf **Ja**, wenn Sie mit der inkrementellen Installation nachfolgender Programmversionen einverstanden sind, falls das für die Installation der ausgewählten Updates erforderlich ist. Klicken Sie auf **Nein**, wenn Sie Anwendungen auf eine geradlinige Weise aktualisieren möchten, ohne nachfolgende Versionen zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

   Daraufhin wird der Assistent für die Erstellung einer Aufgabe Programm-Updates installieren und Schwachstellen schließen gestartet. Folgen Sie den Schritten des Assistenten.

8. Wählen Sie auf der Seite **Methode zum Neustart des Betriebssystems** des Assistenten die Aktion aus, die ausgeführt werden soll, wenn das Betriebssystem auf dem Client-Gerät nach dem Vorgang neu gestartet werden muss:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

   - **Gerät neu starten**

     Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen alle (Min.)**

    Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

    Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neustart nach (Min.)**

    Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

    Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Programmen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

9. Wählen Sie auf der Seite **Geräte auswählen, denen die Aufgabe zugewiesen wird** des Assistenten eine der folgenden Optionen:

   - **Geräte auswählen, die vom Administrationsserver erkannt wurden**

     Die Aufgabe wird einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

     Sie können diese Option beispielsweise für eine Aufgabe zur Installation des Administrationsagenten auf nicht zugeordneten Geräten verwenden.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

     Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

- **Aufgabe einer Administrationsgruppe zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

  Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

  Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

10. Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

    - **Start nach Zeitplan**

      Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

      - **Alle n Stunden**

        Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

        Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

      - **Alle n Tage**

        Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

        Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

      - **Alle n Wochen**

        Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

        Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

      - **Alle n Minuten**

        Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

        Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

11. Geben Sie auf der Seite **Aufgabenname festlegen** des Assistenten den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

12. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

    Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nach Abschluss des Assistenten ist die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** erstellt und wird im Ordner **Aufgaben** angezeigt.

Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Schließen einer Schwachstelle durch Hinzufügen einer Regel zu einer vorhandenen Aufgabe zum Schließen von Schwachstellen

Um eine Schwachstelle durch Hinzufügen einer Regel zu einer vorhandenen Aufgabe zum Schließen von Schwachstellen zu schließen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

2. Wählen Sie die Schwachstelle aus, die Sie schließen möchten.

3. Klicken Sie auf die Schaltfläche **Assistent zum Schließen von Schwachstellen starten**.

   Der Assistent zum Schließen von Schwachstellen wird geöffnet.

   > Das Funktional des Assistenten zum Schließen von Schwachstellen starten ist aktiv, wenn eine Lizenz für die Funktion Schwachstellen- und Patch-Management vorhanden ist.

   Folgen Sie den Schritten des Assistenten.

4. Legen Sie im Fenster **Bestehende Aufgaben zum Schließen von Schwachstellen suchen** die folgenden Einstellungen fest:

   - **Nur Aufgaben anzeigen, die diese Schwachstelle schließen**

     Wenn diese Option aktiviert ist, sucht der Assistent zum Schließen von Schwachstellen nach vorhandenen Aufgaben, mit denen die ausgewählte Schwachstelle geschlossen werden kann.

     Wenn diese Option deaktiviert ist oder die Suche keine anwendbaren Aufgaben ergibt, fordert Sie der Assistent zum Schließen von Schwachstellen auf, eine Regel oder Aufgabe zum Schließen der Schwachstelle zu erstellen.

     Diese Option ist standardmäßig aktiviert.

- **Updates zum Schließen der ausgewählten Schwachstelle freigeben**

  Updates, die eine Schwachstelle schließen, werden für die Installation genehmigt. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

5. Wenn Sie bestehende Aufgaben zum Schließen von Schwachstellen suchen möchten und die Suche einige Aufgaben ergibt, können Sie Eigenschaften dieser Aufgaben anzeigen oder sie manuell starten. Es sind keine weiteren Aktionen erforderlich.

   Anderenfalls klicken Sie auf die Schaltfläche **Regel zum Schließen von Schwachstellen zu bestehender Aufgabe hinzufügen**.

6. Wählen Sie die Aufgabe aus, zu der Sie eine Regel hinzufügen möchten, und klicken Sie dann auf die Schaltfläche **Regel hinzufügen**.

   Sie können auch Eigenschaften der vorhandenen Aufgaben anzeigen, sie manuell starten oder eine neue Aufgabe erstellen.

7. Wählen Sie den Typ der Regel aus, die zur ausgewählten Aufgabe hinzugefügt werden soll, und klicken Sie dann auf die Schaltfläche **Fertigstellen**.

8. Treffen Sie in der angezeigten Eingabeaufforderung Ihre Wahl in Bezug auf die Installation aller vorherigen Anwendungs-Updates. Klicken Sie auf **Ja**, wenn Sie mit der inkrementellen Installation nachfolgender Programmversionen einverstanden sind, falls das für die Installation der ausgewählten Updates erforderlich ist. Klicken Sie auf **Nein**, wenn Sie Anwendungen auf eine geradlinige Weise aktualisieren möchten, ohne nachfolgende Versionen zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

Eine neue Regel zum Schließen der Schwachstelle wird zur vorhandenen Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** hinzugefügt.

Schließen von Schwachstellen in einem isolierten Netzwerk

In diesem Abschnitt werden die Schritte beschrieben, mit denen Sie Schwachstellen in Drittanbieter-Programmen auf verwalteten Geräten schließen können, die mit Administrationsservern ohne Internetzugang verbunden sind.

Szenario: Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk

Sie können Updates installieren und Schwachstellen in Drittanbieter-Programmen beheben, die auf den verwalteten Geräten in einem isolierten Netzwerk installiert sind. Solche Netzwerke umfassen sowohl Administrationsserver als auch die damit verbundenen verwalteten Geräte ohne Internetzugang. Um in so einer Art von Netzwerk Schwachstellen zu schließen, benötigen Sie einen Administrationsserver, der mit dem Internet verbunden ist. Anschließend können Sie Patches (erforderliche Updates) über den Administrationsserver mit Internetzugang herunterladen und diese im nächsten Schritt an isolierte Administrationsserver übertragen.

Mittels Kaspersky Security Center können Sie von Softwareherstellern veröffentlichte Drittanbieter-Software-Updates herunterladen, aber keine Updates für Microsoft-Software auf isolierte Administrationsserver.

Um zu erfahren, wie der Prozess zum Schließen von Schwachstellen in einem isolierten Netzwerk abläuft, lesen Sie sich die Beschreibung und das Schema dieses Prozesses durch.

Erforderliche Vorrausetzungen

Treffen Sie zuerst die folgenden Voraussetzungen:

1. Weisen Sie ein Gerät für die Verbindung mit dem Internet und das Herunterladen von Patches zu. Dieses Gerät wird als Administrationsserver mit Internetzugang angesehen.
2. Installieren Sie Kaspersky Security Center Version 14 oder höher auf den folgenden Geräten:
   - Zugewiesenes Gerät, welches als Administrationsserver mit Internetzugang fungiert
   - Isolierte Geräte, die als Administrationsserver dienen und vom Internet isoliert sind (im Folgenden "isolierte Administrationsserver" genannt)
3. Stellen Sie sicher, dass jeder Administrationsserver über genügend Speicherplatz zum Herunterladen und Speichern von Updates und Patches verfügt.

Schritte

Das Installieren von Updates und das Schließen von Schwachstellen in Drittanbieter-Programmen auf den verwalteten Geräten isolierter Administrationsserver umfasst die folgenden Phasen:

1. **Konfiguration des Administrationsservers mit Internetzugang**

   Bereiten Sie Ihren Administrationsserver mit Internetzugang vor, um Anfragen zu erforderlichen Updates für Drittanbieter-Programme zu bearbeiten und Patches herunterzuladen.

2. **Konfiguration der isolierten Administrationsserver**

   Bereiten Sie Ihre isolierten Administrationsserver vor, damit diese regelmäßig Listen mit erforderlichen Updates erstellen können und die Patches anwenden, die vom Administrationsserver mit Internetzugang heruntergeladen wurden. Nach der Konfiguration versuchen die isolierten Administrationsserver nicht mehr, Patches aus dem Internet herunterzuladen. Stattdessen erhalten sie die Updates mithilfe von Patches.

3. **Übertragen von Patches und Installieren von Updates auf isolierten Administrationsservern**

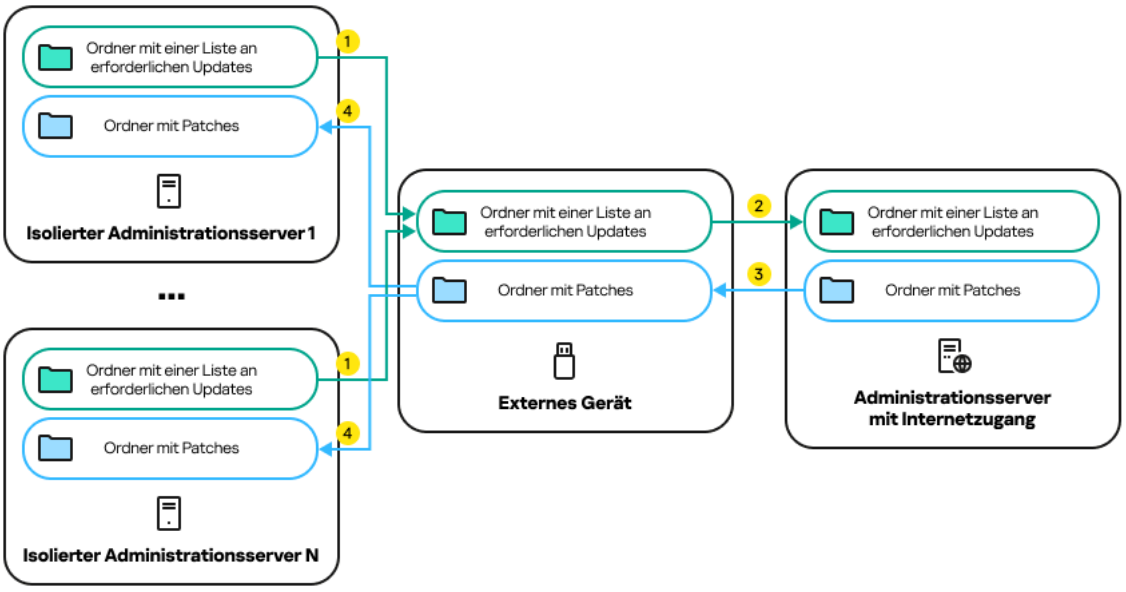
   Nachdem Sie die Konfiguration der Administrationsserver abgeschlossen haben, können Sie die Übertragung der Listen mit erforderlichen Updates und Patches zwischen Administrationsserver mit Internetzugang und isolierten Administrationsservern vornehmen. Anschließend werden unter Verwendung der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die Updates der Patches auf den verwalteten Geräten installiert.

Ergebnisse

Als Ergebnis werden die Updates für Drittanbieter-Programme auf isolierte Administrationsserver übertragen und mithilfe von Kaspersky Security Center auf den verbundenen verwalteten Geräten installiert. Es ist ausreichend, die Administrationsserver einmal zu konfigurieren. Anschließend können Sie Updates beliebig oft erhalten, beispielsweise ein- oder mehrmals am Tag.

Über das Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk

Der Prozess zum Beheben von Schwachstellen in Drittanbietern-Programmen innerhalb eines isolierten Netzwerks ist in der Abbildung dargestellt und nachfolgend beschrieben. Sie können diesen Vorgang regelmäßig wiederholen.



Der Prozess zur Übertragung der Patches und der Liste mit erforderlichen Updates zwischen dem Administrationsserver mit Internetzugang und den isolierten Administrationsservern

Jeder vom Internet isolierte Administrationsserver (im Folgenden als isolierter Administrationsserver bezeichnet) erstellt eine Liste der Updates, die auf den verwalteten Geräten installiert werden müssen, die mit diesem Administrationsserver verbunden sind. Die Liste der erforderlichen Updates wird in einem bestimmten Ordner gespeichert und enthält eine Reihe von Binärdateien. Jede Datei hat einen Namen, der die ID des Patches mit dem erforderlichen Update enthält. Folglich verweist jede Datei in der Liste auf einen bestimmten Patch.

Durch die Verwendung eines externen Gerätes übertragen Sie die Liste mit erforderlichen Updates vom isolierten Administrationsserver auf den zugewiesenen Administrationsserver mit Internetzugang. Anschließend lädt der zugewiesene Administrationsserver Patches aus dem Internet herunter und legt sie in einem separaten Ordner ab.

Wenn alle Patches heruntergeladen sind und sich in dem dafür vorgesehenen Ordner befinden, verschieben Sie die Patches auf all jene isolierten Administrationsserver, von denen Sie eine Liste mit erforderlichen Updates entnommen haben. Sie speichern die Patches in einem eigens dafür auf dem isolierten Administrationsserver erstellten Ordner. Auf diese Weise führt die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* Patches aus und installiert Updates auf den verwalteten Geräten der isolierten Administrationsserver.

Administrationsserver mit Internetzugang konfigurieren, um Schwachstellen in einem isolierten Netzwerk zu schließen

Um das Schließen von Schwachstellen und Übertragen von Patches in einem isolierten Netzwerk vorzubereiten, müssen Sie zunächst den Administrationsserver mit Internetzugang konfigurieren und anschließend die isolierten Administrationsserver konfigurieren.

So konfigurieren Sie einen Administrationsserver mit Internetzugang:

1. Erstellen Sie zwei Ordner auf einer Festplatte, auf welcher der Administrationsserver installiert ist:

   - Einen Ordner für die Liste mit erforderlichen Updates
   - Ordner für Patches

   Sie können diese Ordner beliebig benennen.

2. Gewähren Sie in den erstellten Ordnern unter Verwendung der Standardverwaltungstools des Betriebssystems der Gruppe KLAdmins die Berechtigung zum Ändern.

3. Verwenden Sie das Dienstprogramm "klscflag", um die Pfade zu diesen Ordnern in den Eigenschaften des Administrationsservers festzulegen.

   Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

4. Geben Sie die folgenden Befehle in die Windows-Eingabeaufforderung ein:

   - Um den Pfad zum Patch-Ordner festzulegen:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<Pfad zum Ordner>"`
   - Um den Pfad zum Ordner für die Liste mit erforderlichen Updates festzulegen:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<Pfad zum Ordner>"`

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<Ordner für Patches>"`

5. Verwenden Sie bei Bedarf das Tool "klscflag", um anzugeben, wie oft der Administrationsserver nach neuen Patch-Anforderungen suchen soll:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <Wert in Sekunden>`

   Der Standardwert ist 120 Sekunden.

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Erstellen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Informationen über Patches für Drittanbieter-Programme abzurufen, die auf den verwalteten Geräten installiert sind, und legen Sie anschließend den Aufgabenzeitplan fest.

7. Erstellen Sie die Aufgabe *Schwachstellen schließen*, um Patches anzugeben, die zum Schließen von Schwachstellen in Drittanbieter-Programmen verwendet werden, und legen Sie anschließend den Aufgabenzeitplan fest.

   Starten Sie die Aufgaben manuell, wenn Sie diese früher ausführen möchten, als im Zeitplan angegeben. Die Ausführungsreihenfolge der Aufgaben ist wichtig. Die Aufgabe *Schwachstellen schließen* muss nach der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ausgeführt werden.

8. Starten Sie den Administrationsserver-Dienst neu.

Der Administrationsserver mit Internetzugang ist jetzt bereit, Updates herunterzuladen und an isolierte Administrationsserver zu übertragen. Bevor Sie mit dem Schließen von Schwachstellen beginnen, müssen Sie die isolierten Administrationsserver konfigurieren.

Konfigurieren von isolierten Administrationsservern, Schwachstellen in einem isolierten Netzwerk zu schließen

Nachdem Sie die Konfiguration des Administrationsservers mit Internetzugang abgeschlossen haben, bereiten Sie jeden isolierten Administrationsserver in Ihrem Netzwerk vor, damit Sie auf verwalteten Geräten, die mit isolierten Administrationsservern verbunden sind, Schwachstellen schließen und Updates installieren.

Um die isolierten Administrationsserver zu konfigurieren, führen Sie auf jedem Administrationsserver die folgenden Aktionen aus:

1. Aktivieren Sie einen Lizenzschlüssel für die Funktion "Schwachstellen- und Patch-Management" (VAPM).
2. Erstellen Sie zwei Ordner auf einer Festplatte, auf welcher der Administrationsserver installiert ist:
   - Einen Ordner, in dem die Liste mit erforderlichen Updates erscheint
   - Ordner für Patches

   Sie können diese Ordner beliebig benennen.
3. Gewähren Sie in den erstellten Ordnern unter Verwendung der Standardverwaltungstools des Betriebssystems der Gruppe KLAdmins die Berechtigung zum *Ändern*.
4. Verwenden Sie das Dienstprogramm "klscflag", um die Pfade zu diesen Ordnern in den Eigenschaften des Administrationsservers festzulegen.

   Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".
5. Geben Sie die folgenden Befehle in die Windows-Eingabeaufforderung ein:
   - Um den Pfad zum Patch-Ordner festzulegen:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<Pfad zum Ordner>"`
   - Um den Pfad zum Ordner für die Liste mit erforderlichen Updates festzulegen:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<Pfad zum Ordner>"`

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<Ordner für Patches>"`
6. Verwenden Sie bei Bedarf das Tool "klscflag", um anzugeben, wie oft der isolierte Administrationsserver nach neuen Patches suchen soll:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <Wert in Sekunden>`

   Der Standardwert ist 120 Sekunden.

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`
7. Verwenden Sie bei Bedarf das Tool "klscflag", um die SHA256-Hashes der Patches zu berechnen:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Wenn Sie diesen Befehl eingeben, können Sie sicherstellen, dass die Patches während der Übertragung auf den isolierten Administrationsserver nicht verändert wurden und dass Sie die richtigen Patches mit den erforderlichen Updates erhalten haben.

Standardmäßig berechnet Kaspersky Security Center keine SHA256-Hashes für Patches. Nachdem der isolierte Administrationsserver die Patches erhalten hat, berechnet Kaspersky Security Center bei aktivierter Option deren Hashes und vergleicht die erfassten Werte mit den Hashes, die in der Administrationsserver-Datenbank gespeichert sind. Wenn der berechnete Hash nicht mit dem Hash in der Datenbank übereinstimmt, wird ein Fehler gemeldet und Sie müssen den inkorrekten Patch ersetzen.

8. Erstellen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Informationen über Patches für Drittanbieter-Programme abzurufen, die auf den verwalteten Geräten installiert sind, und legen Sie anschließend den Aufgabenzeitplan fest.

9. Erstellen Sie die Aufgabe *Schwachstellen schließen*, um Patches anzugeben, die zum Schließen von Schwachstellen in Drittanbieter-Programmen verwendet werden, und legen Sie anschließend den Aufgabenzeitplan fest.

   Starten Sie die Aufgaben manuell, wenn Sie diese früher ausführen möchten, als im Zeitplan angegeben. Die Ausführungsreihenfolge der Aufgaben ist wichtig. Die Aufgabe *Schwachstellen schließen* muss nach der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ausgeführt werden.

10. Starten Sie den Administrationsserver-Dienst neu.

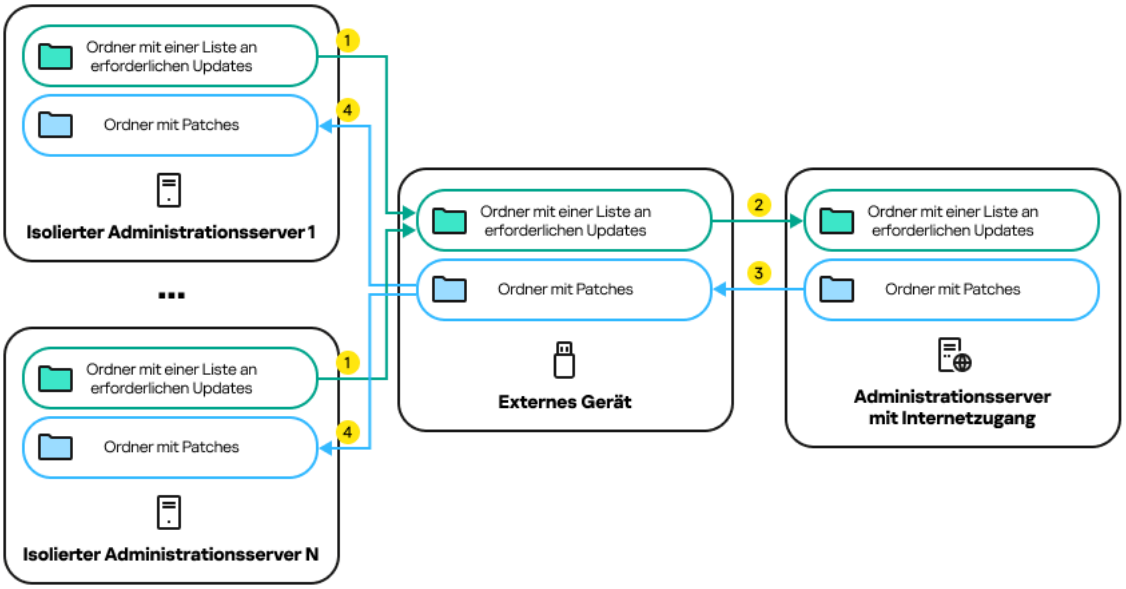
Nachdem Sie alle Administrationsserver konfiguriert haben, können Sie die Patches und die Liste mit erforderlichen Updates verschieben und Schwachstellen in Drittanbieter-Programmen auf den verwalteten Geräten im isolierten Netzwerk beheben.

Übertragen von Patches und Installieren von Updates in einem isolierten Netzwerk

Nachdem Sie die Konfiguration der Administrationsserver abgeschlossen haben, können Sie Patches mit erforderlichen Updates vom Administrationsserver mit Internetzugang auf isolierte Administrationsserver übertragen. Sie können Updates beliebig oft übertragen und installieren, z. B. einmal oder mehrmals täglich.

Sie benötigen ein externes Gerät, beispielsweise einen Wechseldatenträger, um Patches und die Liste der erforderlichen Updates zwischen den Administrationsservern zu übertragen. Stellen Sie daher sicher, dass das externe Gerät über genügend Speicherplatz zum Herunterladen und Speichern der Patches verfügt.

Der Prozess zur Übertragung der Patches und der Liste mit erforderlichen Updates ist in der Abbildung dargestellt und wird im Folgenden beschrieben:



Vorgang zur Übertragung von Patches und der Liste mit erforderlichen Updates zwischen dem Administrationsserver mit Internetzugang und den isolierten Administrationsservern

So installieren Sie Updates und schließen Schwachstellen auf verwalteten Geräten, die mit isolierten Administrationsservern verbunden sind:

1. Starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen*, wenn diese noch nicht ausgeführt wird.

2. Verbinden Sie ein externes Gerät mit einem der isolierten Administrationsserver.

3. Erstellen Sie zwei Ordner auf dem externen Gerät: einen für die Liste mit erforderlichen Updates und einen für Patches. Sie können diese Ordner beliebig benennen.

   Wenn Sie diese Ordner bereits erstellt haben, löschen Sie diese.

4. Kopieren Sie die Liste der erforderlichen Updates von jedem isolierten Administrationsserver und fügen Sie diese Liste auf dem externen Gerät in den Ordner für die Liste mit erforderlichen Updates ein.

   Dadurch führen Sie alle Listen, die von den einzelnen isolierten Administrationsservern erfasst wurden, in einem Ordner zusammen. Dieser Ordner enthält Binärdateien mit den IDs von Patches, die für alle isolierten Administrationsserver erforderlich sind.

5. Verbinden Sie das externe Gerät mit dem Administrationsserver, der Internetzugang hat.

6. Kopieren Sie die Liste mit erforderlichen Updates vom externen Gerät und fügen Sie diese Liste auf dem Administrationsserver mit Internetzugang in den Ordner für die Liste mit erforderlichen Updates ein.

   Auf dem Administrationsserver werden automatisch alle erforderlichen Patches aus dem Internet in den Ordner für Patches heruntergeladen. Dies kann mehrere Stunden dauern.

7. Überprüfen Sie, ob alle erforderlichen Patches heruntergeladen wurden. Gehen Sie dazu wie folgt vor:

   - Überprüfen Sie den Ordner für Patches auf dem Administrationsserver mit Internetzugang. Alle Patches, die in der Liste mit erforderlichen Updates angegeben sind, sollten in den erforderlichen Ordner heruntergeladen werden. Dies ist praktischer, wenn eine kleine Anzahl von Patches benötigt wird.

   - Bereiten Sie ein spezielles Skript (z. B. ein Shell-Skript) vor. Wenn Sie eine große Anzahl von Patches erhalten, ist es schwierig, selbst zu überprüfen, ob alle Patches heruntergeladen wurden. In solchen Fällen ist es besser, die Prüfung zu automatisieren.

8. Kopieren Sie die Patches vom Administrationsserver mit Internetzugang und fügen Sie die Patches in den entsprechenden Ordner auf Ihrem externen Gerät ein.

9. Übertragen Sie die Patches auf jeden der isolierten Administrationsserver. Legen Sie die Patches in einem dafür vorgesehenen Ordner ab.

Als Ergebnis erstellt jeder isolierte Administrationsserver eine aktuelle Liste mit Updates, die für jene verwalteten Geräte erforderlich sind, die mit dem aktuellen Server verbunden sind. Nachdem der Administrationsserver mit Internetzugang die Liste mit erforderlichen Updates erhalten hat, lädt der Administrationsserver die Patches aus dem Internet herunter. Wenn diese Patches auf isolierte Administrationsserver gelangen, verarbeitet die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* diese Patches. Auf diese Weise werden Updates auf verwalteten Geräten installiert und Schwachstellen in Drittanbieter-Programmen behoben.

Wenn die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ausgeführt wird, starten Sie das Gerät des Administrationsservers nicht neu und führen Sie nicht die Aufgabe *Backup der Daten des Administrationsservers anlegen* aus (sie führt ebenfalls zu einem Neustart). Dadurch wird die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* unterbrochen und die Updates werden nicht installiert. In diesem Fall müssen Sie diese Aufgabe manuell neu starten oder warten, bis die Aufgabe nach dem festgelegten Zeitplan gestartet wird.

Option zum Übertragen von Patches und Installieren von Updates in einem isolierten Netzwerk deaktivieren

Sie können die Übertragung von Patches auf isolierten Administrationsservern deaktivieren. Dies kann nützlich sein, wenn Sie einen oder mehrere Administrationsserver aus dem isolierten Netzwerk herausnehmen möchten. Sie können dadurch die Anzahl der Patches und die Zeit für deren Download reduzieren.

So deaktivieren Sie die Option, Patches auf isolierten Administrationsservern zu übertragen:

1. Wenn Sie alle Administrationsserver aus der Isolation nehmen möchten, löschen Sie in den Eigenschaften des Administrationsservers mit Internetzugang die Pfade zu den Ordnern für die Patches sowie für die Liste der erforderlichen Updates. Überspringen Sie diesen Schritt, wenn Sie einige Administrationsserver in einem isolierten Netzwerk behalten möchten.

   Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

   Geben Sie die folgenden Befehle in die Eingabeaufforderung ein:

   - So löschen Sie den Pfad des Ordners für Patches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

   - So löschen Sie den Pfad des Ordners für die Liste mit erforderlichen Updates:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Starten Sie den Dienst des Administrationsservers neu, wenn Sie die Pfade zu den Ordnern auf diesem Administrationsserver gelöscht haben.

3. Löschen Sie in den Eigenschaften jedes Administrationsservers, den Sie aus der Isolation nehmen möchten, die Pfade zu den Ordnern für die Patches und für die Liste der erforderlichen Updates.

   Geben Sie die folgenden Befehle mit Administratorrechten in die Windows-Eingabeaufforderung ein:

   - Um den Pfad des Ordners für Patches zu löschen:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""`

   - So löschen Sie den Pfad des Ordners für die Liste mit erforderlichen Updates:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""`

4. Starten Sie den Dienst von jedem Administrationsserver neu, auf dem Sie die Pfade zu den Ordnern gelöscht haben.

Wenn Sie den Administrationsserver mit Internetzugang neu konfiguriert haben, erhalten Sie über Kaspersky Security Center keine Patches mehr. Wenn Sie beispielsweise nur einige isolierte Administrationsserver neu konfiguriert haben, um diese aus dem isolierten Netzwerk entfernen, werden Sie die Patches nur für die verbleibenden isolierten Administrationsserver erhalten.

Wenn Sie zukünftig die Behebung von Schwachstellen auf deaktivierten isolierten Administrationsservern aktivieren möchten, müssen Sie diese Administrationsserver und den Administrationsserver mit Internetzugang erneut konfigurieren.

Ignorieren von Schwachstellen in Programmen

Sie können Korrekturen für Software-Schwachstellen ignorieren. Gründe für das Ignorieren von Schwachstellen in Programmen können sein:

- Sie betrachten die Software-Schwachstelle nicht als kritisch für Ihr Unternehmen.
- Sie vermuten, dass durch das Schließen von Software-Schwachstellen die Daten des Programms beschädigt werden können, welches das Schließen von Schwachstellen erforderlich macht.
- Sie sind sicher, dass die Software-Schwachstelle keine Gefahr für das Netzwerk Ihres Unternehmens darstellt, da Sie andere Maßnahmen ergriffen haben, um Ihre verwalteten Geräte zu schützen.

Sie können eine Software-Schwachstelle auf allen verwalteten Geräten oder nur auf ausgewählten verwalteten Geräten ignorieren.

Um eine Schwachstelle im Programm auf allen verwalteten Geräten zu ignorieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

   Im Arbeitsbereich des Ordners wird die Liste von Schwachstellen in Programmen angezeigt, die der auf den Client-Geräten installierte Administrationsagent gefunden hat.

2. Wählen Sie die Schwachstelle aus, die Sie ignorieren möchten.

3. klicken Sie mit der rechten Maustaste auf die Schwachstelle und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster der Schwachstelle wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Schwachstelle ignorieren**.

5. Klicken Sie auf die Schaltfläche **OK**.

   Das Fenster mit den Eigenschaften der Schwachstelle im Programm wird geschlossen.

Die Schwachstelle im Programm wird auf allen verwalteten Geräten ignoriert.

Um eine Schwachstelle im Programm auf dem ausgewählten verwalteten Gerät zu ignorieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftenfenster des ausgewählten verwalteten Gerätes und wählen Sie den Abschnitt **Schwachstellen in Programmen** aus.

2. Wählen Sie eine Software-Schwachstelle aus.

3. Ignorieren Sie die ausgewählte Schwachstelle.

Die Software-Schwachstelle wird auf dem ausgewählten Gerät ignoriert.

Die ignorierte Software-Schwachstelle wird im Rahmen der Aufgabe *Schwachstellen schließen* oder *Erforderliche Updates installieren und Schwachstellen schließen* nicht behoben. Mithilfe eines Filters können Sie ignorierte Software-Schwachstellen aus der Liste der Schwachstellen ausschließen.

Auswählen von Benutzerkorrekturen für Schwachstellen in Programmen von Drittanbietern

Zur Verwendung der Aufgabe *Schwachstellen schließen* müssen Sie die Programm-Updates manuell angeben, mit denen die in den Aufgabeneinstellungen angegeben Schwachstellen in den Drittanbieter-Programmen behoben werden sollen. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Software von Microsoft und individuelle Korrekturen für andere Drittanbieter-Programme. *individuelle Korrekturen* sind Programm-Updates zum Beheben von Schwachstellen, die vom Administrator manuell für die Installation ausgewählt werden.

So wählen Sie Benutzerkorrekturen für Schwachstellen in Software von Drittanbietern aus:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

   Im Arbeitsbereich des Ordners wird die Liste von Schwachstellen in Programmen angezeigt, die der auf den Client-Geräten installierte Administrationsagent gefunden hat.

2. Wählen Sie die Schwachstelle aus, für die Sie eine individuelle Korrektur hinzufügen möchten.

3. klicken Sie mit der rechten Maustaste auf die Schwachstelle und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster der Schwachstelle wird geöffnet.

4. Klicken Sie im Abschnitt **Benutzerdefinierte und andere Patches** auf **Hinzufügen**.

   Eine Liste der verfügbaren Installationspakete wird angezeigt. Die Liste der angezeigten Installationspakete entspricht der Liste unter **Remote-Installation** → **Installationspakete**. Wenn Sie kein Installationspaket erstellt haben, das eine benutzerdefinierte Korrektur für die ausgewählte Schwachstelle enthält, können Sie das Paket jetzt mithilfe des "Assistenten für das Erstellen eines Installationspakets" erstellen.

5. Wählen Sie ein Installationspaket (bzw. Pakete) aus, in dem eine benutzerdefinierte Korrektur (bzw. benutzerdefinierte Korrekturen) für die Schwachstelle in der Drittanbieter-Software enthalten ist.

6. Klicken Sie auf die Schaltfläche **OK**.

Die Installationspakete, die Benutzerkorrekturen für die Software-Schwachstelle enthalten, werden angegeben. Bei Ausführung der Aufgabe *Schwachstellen schließen*, wird das Installationspaket installiert und die Software-Schwachstelle wird behoben.

Regeln zur Installation von Updates

Beim Schließen von Schwachstellen in Apps müssen Sie Regeln für die Installation von Updates festlegen. Diese Regeln bestimmen, welche Updates installiert und welche Schwachstellen geschlossen werden.

Die genauen Einstellungen hängen davon ab, ob Sie eine Regel für Updates von Microsoft-Apps, von Drittanbieter-Apps (Apps, von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden) oder von allen Apps erstellen möchten. Beim Erstellen einer Regel für Microsoft-Apps oder Drittanbieter-Apps können Sie bestimme Programme und Programmversionen auswählen, für die Sie Updates installieren möchten. Beim Erstellen einer Regel für alle Programme, können Sie bestimmte Updates, die Sie installieren möchten, und Schwachstellen, die Sie mittels Installation von Updates schließen möchten, auswählen.

Um eine neue Regel für Updates aller Programme zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite **Einstellungen** des Assistenten für das Erstellen einer Aufgabe auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Schritten des Assistenten.

2. Wählen Sie auf der Seite **Regeltyp** die Option **Regel für alle Updates**.

3. Verwenden Sie auf der Seite **Allgemeine Kriterien** die Dropdown-Listen, um die folgenden Einstellungen festzulegen:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.

     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.

     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Updates** die Updates aus, die installiert werden sollen:

   - **Alle relevanten Updates installieren**

     Installieren Sie alle Programm-Updates, von denen die im Assistenten auf der Seite **Allgemeine Kriterien** aufgeführten Kriterien erfüllt werden. Standardmäßig ausgewählt.

   - **Nur Updates aus der Liste installieren**

     Es werden nur Programm-Updates installiert, die Sie in der Liste manuell auswählen. Diese Liste enthält alle verfügbaren Programm-Updates.

     Sie können beispielsweise in den folgenden Fällen bestimmte Updates auswählen: um deren Installation in einer Testumgebung zu überprüfen, um nur kritische Programme zu aktualisieren oder um nur bestimmte Programme zu aktualisieren.

     - **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

       Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

       Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

       Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

       Diese Option ist standardmäßig aktiviert.

5. Wählen Sie auf der Seite **Schwachstellen** jene Schwachstellen aus, die durch die Installation der ausgewählten Updates geschlossen werden:

   - **Alle Schwachstellen schließen, die den übrigen Kriterien entsprechen**

     Beheben Sie alle Schwachstellen, welche die Kriterien auf der Seite **Allgemeine Kriterien** des Assistenten erfüllen. Standardmäßig ausgewählt.

   - **Nur Schwachstellen aus der Liste schließen**

     Es werden nur Schwachstellen geschlossen, die Sie manuell aus der Liste auswählen. Diese Liste enthält alle gefundenen Schwachstellen.

     Sie können beispielsweise in den folgenden Fällen bestimmte Schwachstellen auswählen: um deren Schließen in einer Testumgebung zu überprüfen, um Schwachstellen nur in kritischen Apps zu schließen oder um Schwachstellen nur in bestimmten Programmen zu aktualisieren.

6. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie erstellen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem der Assistent für das Erstellen einer Regel abgeschlossen ist, wird die neue Regel erstellt und im Feld **Regeln für die Installation von Updates festlegen** des Assistent für das Erstellen einer Aufgabe angezeigt.

Um eine neue Regel für Updates von Microsoft-Programmen zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite **Einstellungen** des Assistenten für das Erstellen einer Aufgabe auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Schritten des Assistenten.

2. Wählen Sie auf der Seite **Regeltyp** die Option **Regel für Windows-Updates**.

3. Geben Sie auf der Seite **Allgemeine Kriterien** die folgenden Einstellungen an:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.
     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.
     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

   - **Schwachstellen schließen, deren MSRC-Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Anwendungen** die Programme und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Wählen Sie auf der Seite **Update-Kategorien** die Kategorien von Updates aus, die installiert werden sollen. Diese Kategorien entsprechen den Kategorien im Microsoft-Update-Katalog. Standardmäßig sind alle Kategorien ausgewählt.

6. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie erstellen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem der Assistent für das Erstellen einer Regel abgeschlossen ist, wird die neue Regel erstellt und im Feld **Regeln für die Installation von Updates festlegen** des Assistent für das Erstellen einer Aufgabe angezeigt.

Um eine neue Regel für Updates von Drittanbieter-Apps zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite **Einstellungen** des Assistenten für das Erstellen einer Aufgabe auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Schritten des Assistenten.

2. Wählen Sie auf der Seite **Regeltyp** die Option **Regel für Updates von Drittherstellern**.

3. Geben Sie auf der Seite **Allgemeine Kriterien** die folgenden Einstellungen an:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.

     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.

     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Programme** die Apps und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie erstellen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem der Assistent für das Erstellen einer Regel abgeschlossen ist, wird die neue Regel erstellt und im Feld **Regeln für die Installation von Updates festlegen** des Assistent für das Erstellen einer Aufgabe angezeigt.

Programmgruppen

In diesem Abschnitt werden Vorgänge beschrieben, die für Gruppen von auf Geräten installierten Programmen vorgesehen sind.

Programmkategorien erstellen

Kaspersky Security Center ermöglicht das Erstellen von Programmkategorien der auf den Geräten installierten Programme.

Programmkategorien können auf eine der folgenden Weise erstellt werden:

- Der Administrator gibt einen Ordner an, dessen ausführbaren Dateien in die gewählte Kategorie aufgenommen werden.
- Der Administrator gibt ein Gerät an, dessen ausführbaren Dateien in die gewählte Kategorie aufgenommen werden.
- Der Administrator gibt Kriterien an, nach denen Programme in die gewählte Kategorie aufgenommen werden.

Wenn eine Programmkategorie erstellt wurde, kann der Administrator für diese Kategorie Regeln festlegen. Die Regeln legen das Verhalten der Programme fest, die zur gewählten Kategorie gehören. Der Start von Programmen, die zu dieser Kategorie gehören, kann beispielsweise verboten oder erlaubt sein.

Programmstart auf den Geräten verwalten

Kaspersky Security Center ermöglicht die Verwaltung des Programmstarts auf Geräten im Modus "Allow-Liste". Eine ausführliche Beschreibung finden Sie in der Online-Hilfe für Kaspersky Endpoint Security für Windows. Im Modus "Allow-Liste" können auf den festgelegten Geräten nur solche Programme gestartet werden, die zu den angegebenen Kategorien gehören. Der Administrator kann sich Ergebnisse der statischen Analyse der Regeln für den Programmstart auf Geräten nach jedem Benutzer anzeigen lassen.

Inventarisierung von auf Geräten installierten Programmen

Kaspersky Security Center ermöglicht es Ihnen, eine Inventarisierung von Software auf Windows- und Linux-Geräten durchzuführen. Der Administrationsagent ruft Informationen über alle auf dem Gerät installierten Programme ab. Die bei der Inventarisierung gesammelten Daten werden im Arbeitsbereich des Ordners **Programm-Registry** angezeigt. Der Administrator kann sich ausführliche Informationen zu jedem Programm, einschließlich Version und Hersteller, anzeigen lassen.

Die Anzahl ausführbarer Dateien, die von einem Gerät erhalten werden, darf 150.000 nicht überschreiten. Wenn diese Beschränkung erreicht ist, kann Kaspersky Security Center keinen neuen Daten mehr empfangen.

Lizenzierte Programmgruppen verwalten

Kaspersky Security Center ermöglicht Ihnen, lizenzierte Programmgruppen zu erstellen. Zur lizenzierten Programmgruppe gehören Programme, welche die vom Administrator festgelegten Kriterien erfüllen. Der Administrator kann folgende Kriterien für lizenzierte Programmgruppen angeben:

- Programmname
- Programmversion
- Name des Herstellers
- Programm-Tag

Programme, die einem oder mehreren Kriterien entsprechen, werden automatisch in die Gruppe aufgenommen. Um eine lizenzierte Programmgruppe zu erstellen, muss mindestens ein Kriterium für die Aufnahme von Programmen in diese Gruppe angegeben werden.

Jede lizenzierte Programmgruppe hat einen eigenen Lizenzschlüssel. Der Lizenzschlüssel einer lizenzierten Programmgruppe legt fest, wie viele Installationen für die Programme in dieser Gruppe maximal erlaubt sind. Wird die maximale Anzahl der durch den Lizenzschlüssel vorgesehenen Installationen überschritten, so wird auf dem Administrationsserver ein Informationsereignis aufgezeichnet. Der Administrator kann ein Ablaufdatum für den Lizenzschlüssel angeben. An diesem Datum wird auf dem Administrationsserver ein Informationsereignis registriert.

Informationen über ausführbare Dateien anzeigen

Kaspersky Security Center empfängt alle Informationen zu ausführbaren Dateien, die seit der Installation des Betriebssystems auf den Geräten gestartet wurden. Die gesammelten Informationen zu ausführbaren Dateien werden im Programmhauptfenster im Arbeitsbereich des Ordners **Ausführbare Dateien** angezeigt.

Programmkontrolle zur Verwaltung ausführbarer Dateien verwenden

Sie können die Programmkontrolle verwenden, um das Starten ausführbarer Dateien auf Benutzergeräten zu erlauben oder blockieren. Die Programmkontrolle unterstützt sowohl Windows- als auch Linux-basierte Betriebssysteme.

Für Linux-basierte Betriebssysteme ist die Programmkontrolle ab Kaspersky Endpoint Security 11.2 für Linux verfügbar. Darüber hinaus ist die Komponente für Kaspersky Embedded Systems Security für Windows ab Version 3.0 verfügbar.

Erforderliche Vorrausetzungen

- Kaspersky Security Center ist in Ihrer Organisation bereitgestellt.
- Die Richtlinie von Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security für Linux wurde erstellt und ist aktiv.
- Die Richtlinie von Kaspersky Embedded Systems Security für Windows oder Kaspersky Endpoint Security für Linux wurde erstellt und ist aktiv.

Schritte

Die Nutzung der Programmkontrolle erfolgt schrittweise:

1. **Erstellen und Anzeigen der Liste der ausführbaren Dateien auf Client-Geräten**

   Dieser Schritt unterstützt Sie dabei, herauszufinden, welche ausführbaren Dateien sich auf verwalteten Geräten befinden. Öffnen Sie die Liste der ausführbaren Dateien und vergleichen Sie diese mit den Listen der zulässigen und verbotenen ausführbaren Dateien. Die Einschränkungen zur Nutzung ausführbarer Dateien können sich auf die Informationssicherheitsrichtlinien des Unternehmens beziehen.

   Anleitung:

   - Verwaltungskonsole: Inventarisierung der ausführbaren Dateien
   - Kaspersky Security Center Web Console: Abrufen und Anzeigen einer Liste der auf Client-Geräten gespeicherten ausführbaren Dateien

2. **Erstellen von Kategorien für ausführbare Dateien, die in Ihrem Unternehmen verwendet werden**

   Analysieren Sie die Listen der ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind. Erstellen Sie basierend auf der Analyse Kategorien für ausführbare Dateien. Es wird empfohlen, die Kategorie "Arbeitsanwendung" zu erstellen, welche die Standardauswahl an ausführbaren Dateien enthält, die in Ihrem Unternehmen verwendet werden. Wenn von verschiedenen Sicherheitsgruppen unterschiedliche ausführbare Dateien verwendet werden, können Sie für jede Sicherheitsgruppe eine separate Kategorie erstellen.

   Anleitung:

   - Verwaltungskonsole: Manuell zu erweiternde Programmkategorie erstellen, Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen, Programmkategorie mit ausführbaren Dateien aus einem bestimmten Ordner erstellen.
   - Kaspersky Security Center Web Console: Manuell zu erweiternde Programmkategorie erstellen, Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen, Programmkategorie mit ausführbaren Dateien aus einem bestimmten Ordner erstellen.

3. **Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security**

   Konfigurieren Sie die Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security anhand der Kategorien, die Sie im vorherigen Schritt erstellt haben.

   Anleitung:

   - Verwaltungskonsole: Verwaltung des Programmstarts auf Client-Geräten anpassen
   - Kaspersky Security Center Web Console: Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows

4. **Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Embedded Systems Security**

   Konfigurieren Sie die Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Embedded Systems Security für Windows anhand der Programmkategorien, die Sie bereits erstellt haben. Weitere Informationen über die Programmkontrolle finden Sie in der Hilfe zu Kaspersky Embedded Systems Security für Windows oder in der Hilfe zu Kaspersky Embedded Systems Security für Linux.

   Wenn Sie eine große Anzahl an Regeln verwenden, kann beim Laden der Richtlinie ein Fehler auftreten. Sie können für die Anforderung die maximale Größe in Bytes mithilfe der folgenden Befehle erhöhen:

   - Für die Anforderung mittels JSON:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
     ```

- Für die Anforderung mittels HTTP:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  Wobei `<max_request_size>` für die maximale Größe der Anforderung in Byte steht (z. B. `200000000`).

5. **Aktivieren der Komponente "Programmkontrolle" im Test-Modus**

   Um sicherzustellen, dass die Regeln der Programmkontrolle nicht die für die Benutzerarbeit erforderlichen ausführbaren Dateien blockieren, wird empfohlen, das Testen der Regeln der Programmkontrolle zu aktivieren und ihre Funktionsweise nach dem Erstellen neuer Regeln zu analysieren. Bei aktiviertem Test-Modus blockiert Kaspersky Embedded Systems Security für Windows keine ausführbaren Dateien, deren Start durch die Regeln der Programmkontrolle unzulässig ist. Stattdessen werden Benachrichtigungen über deren Start an den Administrationsserver gesendet.

   Es wird empfohlen, beim Testen von Regeln der Programmkontrolle die folgenden Aktionen auszuführen:

   - Festlegen des Testzeitraums. Der Testzeitraum kann zwischen mehreren Tagen und zwei Monaten liegen.
   - Untersuchen Sie die Ereignisse, die sich aus dem Testen der Funktionsweise der Programmkontrolle ergeben.

   Anleitung für Kaspersky Security Center Web Console: Konfigurieren der Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows. Folgen Sie dieser Anweisung und aktivieren Sie beim Konfigurieren die Option **Testbetrieb**.

6. **Ändern der Einstellungen für Kategorien der Komponente "Programmkontrolle"**

   Nehmen Sie bei Bedarf Änderungen an den Einstellungen für die Programmkontrolle vor. Auf der Grundlage der Testergebnisse können Sie einer zu erweiternden Kategorie manuell ausführbare Dateien hinzufügen, die sich auf Ereignisse der Programmkontrolle beziehen.

   Anleitung:

   - Verwaltungskonsole: Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen
   - Kaspersky Security Center Web Console: Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

7. **Anwenden der Regeln der Programmkontrolle im Funktionsmodus**

   Nachdem die Regeln der Programmkontrolle getestet wurden und die Konfiguration der Kategorien abgeschlossen ist, können Sie die Regeln der Programmkontrolle im Ausführungsmodus anwenden.

   Anleitung für Kaspersky Security Center Web Console: Konfigurieren der Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows. Folgen Sie dieser Anweisung und deaktivieren Sie beim Konfigurieren die Option **Testbetrieb**.

8. **Überprüfen der Konfiguration der Programmkontrolle**

   Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

   - Erstellen von Kategorien für ausführbare Dateien
   - Konfigurieren der Programmkontrolle unter Verwendung der Kategorien
   - Anwenden der Regeln der Programmkontrolle im Funktionsmodus

Ergebnisse

Wenn das Szenario abgeschlossen ist, wird der Start der ausführbaren Dateien auf den verwalteten Geräten gesteuert. Die Benutzer können nur jene ausführbaren Dateien starten, die in Ihrem Unternehmen erlaubt sind. Im Unternehmen verbotene ausführbare Dateien können nicht gestartet werden.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen

Sie können die Liste der ausführbaren Dateien, die sich auf den Client-Geräten befinden, auf eine der folgenden Arten abrufen:

- Indem Sie in der Richtlinie von Kaspersky Endpoint Security die Benachrichtigungen über gestartete Anwendungen aktivieren.
- Indem Sie eine Inventarisierungsaufgabe erstellen.

In der Richtlinie von Kaspersky Endpoint Security die Benachrichtigungen über gestartete Anwendungen aktivieren

So aktivieren Sie die Benachrichtigungen über gestartete Anwendungen:

1. Öffnen Sie die Einstellungen der Richtlinie von Kaspersky Endpoint Security und wechseln Sie anschließend zu **Allgemeine Einstellungen → Berichte und Speicher**.
2. Aktivieren Sie in der Einstellungsgruppe **Datenübertragung an den Administrationsserver** das Kontrollkästchen **Über gestartete Anwendungen** und speichern Sie die Änderungen.

Wenn ein Benutzer versucht, ausführbare Dateien zu starten, werden Informationen über diese Dateien zur Liste der ausführbaren Dateien auf einem Client-Gerät hinzugefügt. Kaspersky Endpoint Security sendet diese Informationen an den Administrationsagenten, welcher sie anschließend an den Administrationsserver weiterleitet.

Eine Inventarisierungsaufgabe erstellen

Die Funktion zum Inventarisieren ausführbarer Dateien ist für die folgenden Programme verfügbar:

- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security für Linux ab Version 11.2
- Kaspersky Security for Virtualization 4.0 Light Agent und höhere Versionen

Sie können die Auslastung der Datenbank verringern und gleichzeitig Informationen über die installierten Anwendungen erhalten. Um Speicherplatz zu sparen, führen Sie eine Bestandsaufnahme auf den Referenzgeräten durch, die mit einem Standardpaket an Software ausgestattet sind. Die empfohlene Anzahl an Geräten beträgt 1-3.

Es wird dringend davon abgeraten, die Inventarisierungsaufgabe auszuführen, wenn Sie eine der folgenden Datenbanken verwenden: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (alle Editionen).

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Klicken Sie im Arbeitsbereich des Ordners **Aufgaben** auf die Schaltfläche **Neue Aufgabe**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten den Aufgabentyp **Kaspersky Endpoint Security** und den Aufgabentyp **Inventarisierung**. Klicken Sie auf die Schaltfläche **Weiter**.
4. Folgen Sie den weiteren Schritten des Assistenten.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe **Inventarisierung** erstellt und angepasst. Wenn Sie möchten, können Sie die Einstellungen für die erstellte Aufgabe ändern. Daraufhin wird die neu erstellte Aufgabe in der Aufgabenliste angezeigt. Wenn Sie möchten, können Sie die Einstellungen für die erstellte Aufgabe ändern.

Weitere Informationen zur Inventarisierungsaufgabe finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent

Nach Ausführung der Aufgabe **Inventarisierung** wird die Liste der auf verwalteten Geräten gespeicherten ausführbaren Dateien erstellt und Sie können die Liste anzeigen.

Im Rahmen einer Inventarisierung können die Dateien folgender Formate erkannt werden (in Abhängigkeit Ihrer gewählten Optionen in den Aufgabeneigenschaften): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR und HTML.

Anzeigen der Liste mit ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind.

Um sich die Liste aller auf den Client-Geräten gespeicherten ausführbaren Dateien anzeigen zu lassen, gehen Sie wie folgt vor:

Rufen Sie in der Konsolenstruktur den Abschnitt **Erweitert** → **Anwendungsverwaltung** → **Ausführbare Dateien** auf.

Bei Bedarf können Sie eine ausführbare Datei von einem verwalteten Gerät an das Gerät mit installierter Verwaltungskonsole senden.

So senden Sie eine ausführbare Datei:

1. Rufen Sie in der Konsolenstruktur den Abschnitt **Erweitert** → **Anwendungsverwaltung** → **Ausführbare Dateien** auf.
2. Klicken Sie auf den Link der ausführbaren Datei, die Sie an das Gerät mit installierter Verwaltungskonsole senden möchten.
3. Wechseln Sie im nächsten Fenster zum Abschnitt **Geräte** und aktivieren Sie anschließend das Kontrollkästchen des verwalteten Geräts, von dem Sie die ausführbare Datei senden möchten.

   Stellen Sie vor dem Absenden der ausführbaren Datei durch das Aktivieren des Kontrollkästchens **Verbindung mit Administrationsserver nicht trennen** sicher, dass das verwaltete Gerät eine direkte Verbindung zum Administrationsserver besitzt.
4. Klicken Sie auf die Schaltfläche **Senden**, wählen Sie den Zielordner aus und klicken Sie anschließend auf **OK**.

Die ausgewählte ausführbare Datei heruntergeladen, um sie anschließend an das Gerät mit der installierten Verwaltungskonsole weiterzuleiten.

Erstellen von Programmkategorien für Richtlinien von Kaspersky Endpoint Security für Windows

Sie können Programmkategorien Richtlinien von Kaspersky Endpoint Security für Windows aus dem Ordner **Programmkategorien** und aus dem Fenster **Eigenschaften** einer Richtlinie von Kaspersky Endpoint Security für Windows erstellen.

*Um eine Programmkategorie für eine Richtlinie von Kaspersky Endpoint Security aus dem Ordner **Programmkategorien** zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Programmverwaltung** → **Programmkategorien** aus.
2. Klicken Sie im Arbeitsbereich des Ordners **Programmkategorien** auf die Schaltfläche **Neue Kategorie**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet.

3. Wählen Sie auf der Seite **Kategorietyp** den Typ der Benutzerkategorie aus:

   - **Manuell zu erweiternde Kategorie**. Legen Sie die Kriterien fest, gemäß denen die ausführbaren Dateien der erstellten Kategorie zugewiesen werden.
   - **Automatisch zu erweiternde Kategorie**. Geben Sie den Ordner an, aus dem die ausführbaren Dateien automatisch der erstellten Kategorie zugewiesen werden sollen.

     Wenn Sie eine Kategorie mit automatisch erweiterten Inhalten erstellen, inventarisiert die Anwendung die folgenden Dateitypen: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX und SCR.

   - **Kategorie für ausführbare Dateien von ausgewählten Geräten**. Geben Sie das Gerät an, dessen ausführbare Dateien automatisch der Kategorie zugewiesen werden.

4. Folgen Sie den Anweisungen des Assistenten.

   Wenn der Assistent beendet ist, wird eine benutzerdefinierte Programmkategorie erstellt. Die erstellten Kategorien können mithilfe der Kategorieliste im Arbeitsbereich des Ordners **Programmkategorien** angezeigt werden.

Wenn Sie eine Programmkategorie in eine KLC-Datei exportieren möchten, klicken Sie mit der rechten Maustaste auf den Namen der Kategorie, wählen Sie im Menü **Exportieren** aus, geben Sie im neuen Fenster den Dateinamen an und klicken Sie anschließend auf **Speichern**.

Sie können auch eine Programmkategorie aus dem Ordner **Richtlinien** erstellen.

*Um eine Programmkategorie aus dem Fenster **Eigenschaften** einer Richtlinie von Kaspersky Endpoint Security für Windows zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Richtlinien** eine Richtlinie von Kaspersky Endpoint Security aus, für die Sie eine Kategorie erstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf **Eigenschaften**.
4. Wählen Sie im nächsten Fenster **Eigenschaften** im linken Bereich **Abschnitte** die Option **Sicherheitskontrolle → Programmkontrolle** aus.
5. Treffen Sie im Abschnitt **Programmkontrolle** in den Dropdown-Listen **Kontrollmodus** und **Aktion** Auswahlen für die Allow-Liste oder Deny-Liste und klicken Sie dann auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Regel der Programmkontrolle** wird mit einer Liste von Kategorien geöffnet.
6. Klicken Sie auf die Schaltfläche **Neu erstellen**.
7. Geben Sie den Namen der neuen Kategorie ein und klicken Sie auf **OK**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet.

8. Wählen Sie auf der Seite **Kategorietyp** den Typ der Benutzerkategorie aus:

   - **Manuell zu erweiternde Kategorie**. Legen Sie die Kriterien fest, gemäß denen die ausführbaren Dateien der erstellten Kategorie zugewiesen werden.
   - **Automatisch zu erweiternde Kategorie**. Geben Sie den Ordner an, aus dem die ausführbaren Dateien automatisch der erstellten Kategorie zugewiesen werden sollen.

     Wenn Sie eine Kategorie mit automatisch erweiterten Inhalten erstellen, inventarisiert die Anwendung die folgenden Dateitypen: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX und SCR.

   - **Kategorie für ausführbare Dateien von ausgewählten Geräten**. Geben Sie das Gerät an, dessen ausführbare Dateien automatisch der Kategorie zugewiesen werden.

9. Folgen Sie den Anweisungen des Assistenten.

Wenn der Assistent beendet ist, wird eine benutzerdefinierte Programmkategorie erstellt. Neu erstellte Kategorien werden in der Liste der Kategorien angezeigt.

Die Programmkategorien werden von der Komponente "Programmkontrolle" verwendet, die Bestandteil von Kaspersky Endpoint Security für Windows ist. Die Komponente "Programmkontrolle" ermöglicht dem Administrator, Beschränkungen des Programmstarts auf Client-Geräten einzurichten (z. B. anhand der Programme, die zur ausgewählten Kategorie gehören).

Manuell zu erweiternde Programmkategorie erstellen

Sie können einen Satz von Kriterien als Vorlage für ausführbare Dateien angeben, deren Start Sie in Ihrem Unternehmen zulassen oder blockieren möchten. Basierend auf ausführbaren Dateien, die den Kriterien entsprechen, können Sie eine Programmkategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

Um eine manuell zu erweiternde Programmkategorie zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum aus dem Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Programmkategorien**.
2. Klicken Sie auf die Schaltfläche **Neue Kategorie**.

   Der **Assistent für das Erstellen einer Kategorie** wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie im Assistenten auf der Seite **Kategorietyp** als Typ der Benutzerkategorie die Option **Manuell zu erweiternde Kategorie** aus.
4. Geben Sie im Assistenten auf der Seite **Geben Sie den Namen der Programmkategorie ein** den Namen der neuen Programmkategorie ein.
5. Klicken Sie auf der Seite **Bedingungen für die Aufnahme von Programmen in Kategorien festlegen** auf **Hinzufügen**.

6. Geben Sie in der Dropdown-Liste die erforderlichen Einstellungen an:

- **Aus der Liste ausführbarer Dateien**

  Wenn Sie diese Variante wählen, können Sie die Programme, die in die Kategorie aufgenommen werden sollen, aus der Liste der ausführbaren Dateien des Client-Geräts auswählen.

- **Aus den Dateieigenschaften**

  Wenn Sie diese Variante wählen, können Sie detaillierte Daten ausführbarer Dateien, die in die benutzerdefinierte Programmkategorie aufgenommen werden, manuell bestimmen.

- **Metadaten der Dateien im angegebenen Ordner**

  Geben Sie den Ordner auf dem Client-Gerät an, der die ausführbaren Dateien enthält. Die Metadaten der ausführbaren Dateien, die sich im angegebenen Ordner befinden, werden an den Administrationsserver weitergegeben. Ausführbare Dateien mit denselben Metadaten werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Prüfsummen der Dateien in dem Ordner**

  Wenn Sie diese Option wählen, können Sie einen Ordner auf dem Client-Gerät wählen oder erstellen. Der MD5-Hash der Dateien, die in diesem Ordner enthalten sind, wird an den Administrationsserver weitergegeben. Programme mit demselben Hash werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Zertifikate für die Dateien aus dem Ordner**

  Wenn Sie diese Variante wählen, können Sie einen Ordner auf dem Client-Gerät angeben, der mit Zertifikat signierte ausführbare Dateien enthält. Zertifikate von ausführbaren Dateien werden abgefragt und zu den Kategoriebedingungen hinzugefügt. Ausführbare Dateien, die gemäß dem angegebenen Zertifikat signiert sind, werden zur Benutzerkategorie hinzugefügt.

  > Informationen über Zertifikate können nur aus ausführbaren Dateien im PE-Format (.exe, .dll, .sys) extrahiert werden.

- **Metadaten der Dateien des msi-Installers**

  Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie eine MSI-Installationsdatei angeben. Die Metadaten des Installers werden an den Administrationsserver weitergegeben. Programme, deren Installer-Metadaten mit denen des MSI-Installers übereinstimmen, werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Prüfsummen der Dateien des msi-Installers für das Programm**

  Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie eine MSI-Installationsdatei angeben. Der Hash der Installationsdatei wird an den Administrationsserver weitergegeben. Programme, deren MSI-Installationsdateien in ihrem Hash mit der angegebenen Datei übereinstimmen, werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Aus der KL-Kategorie**

  Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Anwendungen in eine benutzerdefinierte Kategorie die Kategorie für Kaspersky-Anwendungen angeben. Programme, die zur angegebenen Kaspersky-Kategorie gehören, werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Pfad des Programms festlegen (Masken unterstützt)**

  Wenn diese Option ausgewählt ist, können Sie den Pfad der Datei oder des Ordners auf dem Client-Gerät festlegen, der die ausführbaren Dateien enthält, die zur benutzerdefinierten Programmkategorie hinzugefügt werden sollen. Sie können reguläre Ausdrücke wie *C:\path_to_exe** verwenden, etwa: *C:\Programme\Internet Explorer**.

- **Zertifikat aus Datenverwaltung auswählen**

  Wenn Sie diese Option auswählen, können Sie Zertifikate aus der Datenverwaltung angeben. Die Kategoriebedingung entspricht nur den ausführbaren Dateien, die durch das angegebene Zertifikat signiert sind.

  Zertifikate werden zur Datenverwaltung hinzugefügt, wenn Sie eine Inventarisierungsaufgabe erstellt und gestartet haben oder das Kontrollkästchen **Über ausgeführte Anwendungen in der Richtlinie von Kaspersky Endpoint Security** ausgewählt haben. Sie können beide Aktionen ausführen.

- **Datenträgertyp**

  Wenn Sie diese Variante wählen, können Sie einen Datenträgertyp (beliebiger oder Wechseldatenträger) angeben, auf dem das Programm ausgeführt wird. Die auf dem ausgewählten Datenträgertyp ausgeführten Programme werden in die benutzerdefinierte Programmkategorie aufgenommen.

7. Klicken Sie im Assistenten auf der Seite **Programmkategorie wird erstellt** auf **Fertigstellen**.

Kaspersky Security Center verwendet nur Metadaten solcher Dateien, die eine digitale Signatur enthalten. Es ist nicht möglich, eine Kategorie auf Basis von Metadaten von Dateien zu erstellen, die keine digitale Signatur enthalten.

Nach Abschluss des Assistenten wird eine benutzerdefinierte Programmkategorie erstellt, die manuell erweitert wird. Die erstellte Kategorie kann in der Kategorienliste im Arbeitsbereich des Ordners **Programmkategorien** angezeigt werden.

Wenn Sie eine Programmkategorie in eine KLC-Datei exportieren möchten, klicken Sie mit der rechten Maustaste auf den Namen der Kategorie, wählen Sie im Menü **Exportieren** aus, geben Sie im neuen Fenster den Dateinamen an und klicken Sie anschließend auf **Speichern**.

Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen

Sie können ausführbare Dateien von ausgewählten Geräten als Vorlage für ausführbare Dateien verwenden, die Sie zulassen oder blockieren möchten. Basierend auf ausführbaren Dateien von ausgewählten Geräten können Sie eine Programmkategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

So rufen Sie die Liste der ausführbaren Dateien von Geräten ab:

1. Stellen Sie sicher, dass die Richtlinie von Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security für Linux erstellt wurde und aktiv ist. Aktivieren Sie in der Richtlinie die Komponente "Programmkontrolle".

2. Rufen Sie die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien ab.

Um eine Programmkategorie zu erstellen, die ausführbare Dateien von ausgewählten Geräten enthält, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum aus dem Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Programmkategorien**.

2. Klicken Sie auf die Schaltfläche **Neue Kategorie**.

   Der **Assistent für das Erstellen einer Kategorie** wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie Assistenten auf der Seite **Kategorietyp** die **Kategorie für ausführbare Dateien von ausgewählten Geräten** als Typ der Benutzerkategorie.

4. Geben Sie im Assistenten auf der Seite **Geben Sie den Namen der Programmkategorie ein** den Namen der neuen Programmkategorie ein.

5. Klicken Sie im Assistenten auf der Seite **Einstellungen** auf **Hinzufügen**.

6. Wählen Sie mindestens ein Gerät aus, dessen ausführbare Dateien zum Erstellen der Programmkategorie verwendet werden sollen.

7. Geben Sie die folgenden Einstellungen an:

   - **Algorithmus für die Berechnung der Hash-Funktion**

     Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

     SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher unterstützt die Berechnung von SHA256. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows unterstützt.

     Wählen Sie eine der Varianten zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center aus:

     - Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheitsanwendungen dem Programm Kaspersky Endpoint Security 10 Service Pack 2 für Windows oder höher entsprechen, wählen Sie die das Kontrollkästchen **SHA256** aus. Es wird nicht empfohlen, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA256-Hash einer ausführbaren Datei" erstellt wurde. Das kann zum Absturz der Sicherheitsanwendungen führen. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion MD5 verwenden.

     - Wenn in Ihrem Netzwerk niedrigere Versionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows installiert sind, wählen Sie die **MD5-Hash** aus. Für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows kann keine Kategorie hinzugefügt werden, die nach dem MD5-Prüfsummen-Kriterium der ausführbaren Datei erstellt wurde. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion SHA256 verwenden.

     Wenn verschiedene Geräte in Ihrem Netzwerk sowohl niedrigere als auch höhere Versionen von Kaspersky Endpoint Security 10 verwenden, aktivieren Sie die beiden Kontrollkästchen **SHA256** und **MD5-Hash**.

     Standardmäßig ist das Kontrollkästchen **SHA256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)** aktiviert.

Standardmäßig ist das Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)** deaktiviert.

- **Daten mit der Datenverwaltung des Administrationsservers synchronisieren**

  Wählen Sie diese Option, wenn der Administrationsserver die Änderungen in dem bzw. den angegebenen Ordner(n) regelmäßig überprüfen soll.

  Diese Option ist standardmäßig deaktiviert.

  Wenn Sie diese Option aktivieren, geben Sie den Zeitraum (in Stunden) an, in dem die Änderungen in den angegebenen Ordnern überprüft werden sollen. Standardmäßig beträgt das Untersuchungsintervall 24 Stunden.

8. Geben Sie im Assistenten auf der Seite **Filter** die folgenden Einstellungen an:

   - **Dateityp**

     In diesem Abschnitt können Sie den Dateityp angeben, mit dem die Programmkategorie erstellt wird.

     Alle Dateien. Alle Dateien werden beim Erstellen der Kategorie berücksichtigt. Diese Variante ist standardmäßig ausgewählt.

     Nur Dateien, die keiner Programmkategorie entsprechen. Nur Dateien außerhalb der Programmkategorien werden beim Erstellen der Kategorie berücksichtigt.

   - **Ordner**

     In diesem Abschnitt können Sie Ordner auf dem ausgewählten Gerät (bzw. den ausgewählten Geräten) angeben, die Dateien enthalten, mit denen die Programmkategorie erstellt wird.

     Alle Ordner. Alle Ordner werden beim Erstellen der Kategorie berücksichtigt. Diese Variante ist standardmäßig ausgewählt.

     Angegebener Ordner. Nur der angegebene Ordner wird beim Erstellen der Kategorie berücksichtigt. Bei Auswahl dieser Option müssen Sie den Pfad zum Ordner angeben.

9. Klicken Sie im Assistenten auf der Seite **Programmkategorie wird erstellt** auf **Fertigstellen**.

Wenn der Assistent abgeschlossen ist, wird eine Benutzerprogrammkategorie erstellt. Die erstellte Kategorie kann in der Kategorienliste im Arbeitsbereich des Ordners **Programmkategorien** angezeigt werden.

Wenn Sie eine Programmkategorie in eine KLC-Datei exportieren möchten, klicken Sie mit der rechten Maustaste auf den Namen der Kategorie, wählen Sie im Menü **Exportieren** aus, geben Sie im neuen Fenster den Dateinamen an und klicken Sie anschließend auf **Speichern**.

Erstellen einer Programmkategorie mit ausführbaren Dateien aus einem bestimmten Ordner

Sie können die ausführbaren Dateien aus einem bestimmten Ordner als Standard für die ausführbaren Dateien verwenden, die Sie in Ihrem Unternehmen zulassen oder blockieren möchten. Basierend auf den ausführbaren Dateien aus dem ausgewählten Ordner können Sie eine Programmkategorie erstellen und diese verwenden, um die Komponente "Programmkontrolle" anzupassen.

So erstellen Sie eine Programmkategorie, die ausführbare Dateien aus einem bestimmten Ordner enthält:

1. Wählen Sie im Konsolenbaum aus dem Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Programmkategorien**.

2. Klicken Sie auf die Schaltfläche **Neue Kategorie**.

   Der **Assistent für das Erstellen einer Kategorie** wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie im Assistenten auf der Seite **Kategorietyp** die **Kategorie für ausführbare Dateien aus ausgewählten Ordnern** als Typ der Benutzerkategorie.

4. Geben Sie im Assistenten auf der Seite **Geben Sie den Namen der Programmkategorie ein** den Namen der neuen Programmkategorie ein.

5. Klicken Sie im Assistenten auf der Seite **Ordner der Datenverwaltung** auf **Durchsuchen**.

6. Geben Sie den Ordner an, dessen ausführbare Dateien zum Erstellen der Programmkategorie verwendet werden.

7. Passen Sie die folgenden Einstellungen an:

   - **Dynamic Link Libraries (.dll) in diese Kategorie aufnehmen**

     Zur Programmkategorie werden dynamisch verbundene Bibliotheken (dll-Dateien) hinzugefügt und die Komponente "Programmkontrolle" registriert die Aktionen solcher Bibliotheken, die im System gestartet werden. Es ist möglich, dass nach der Aufnahme von dll-Dateien in die Kategorie die Leistung von Kaspersky Security Center sinkt.

     Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

   - **Skriptdateien in diese Kategorie aufnehmen**

     Zur Programmkategorie werden Informationen zu Skripten hinzugefügt und die Skripte werden von der Komponente "Schutz vor Web-Bedrohungen" nicht gesperrt. Es ist möglich, dass nach der Aufnahme von Daten zu Skripten in die Kategorie die Leistung von Kaspersky Security Center sinkt.

     Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

   - **Algorithmus für die Berechnung der Hash-Funktion**: **SHA256 für die Dateien der Kategorie berechnen (unterstützt von Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher) / MD5 für die Dateien der Kategorie berechnen (unterstützt von Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**

     Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

     SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher unterstützt die Berechnung von SHA256. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows unterstützt.

Wählen Sie eine der Varianten zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center aus:

- Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheitsanwendungen dem Programm Kaspersky Endpoint Security 10 Service Pack 2 für Windows oder höher entsprechen, wählen Sie die das Kontrollkästchen **SHA256** aus. Es wird nicht empfohlen, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA256-Hash einer ausführbaren Datei" erstellt wurde. Das kann zum Absturz der Sicherheitsanwendungen führen. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion MD5 verwenden.

- Wenn in Ihrem Netzwerk niedrigere Versionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows installiert sind, wählen Sie die **MD5-Hash** aus. Für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows kann keine Kategorie hinzugefügt werden, die nach dem MD5-Prüfsummen-Kriterium der ausführbaren Datei erstellt wurde. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion SHA256 verwenden.

Wenn verschiedene Geräte in Ihrem Netzwerk sowohl niedrigere als auch höhere Versionen von Kaspersky Endpoint Security 10 verwenden, aktivieren Sie die beiden Kontrollkästchen **SHA256** und **MD5-Hash**.

Standardmäßig ist das Kontrollkästchen **SHA256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)** aktiviert.

Standardmäßig ist das Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)** deaktiviert.

- **Untersuchung des Ordners auf Änderungen erzwingen**

  Wenn diese Option aktiviert ist, erzwingt das Programm regelmäßig eine Prüfung des Ordners für die Erweiterung von Kategorien auf Veränderungen. Das Prüfintervall in Stunden kann im Eingabefeld neben dem Kontrollkästchen eingegeben werden. Standardmäßig beträgt das Intervall für die erzwungene Prüfung 24 Stunden.

  Ist diese Option deaktiviert, erfolgt keine erzwungene Prüfung des Ordners. Der Server greift auf die Dateien im Ordner zu, wenn diese verändert, hinzugefügt oder gelöscht werden.

  Diese Option ist standardmäßig deaktiviert.

8. Klicken Sie im Assistenten auf der Seite **Programmkategorie wird erstellt** auf **Fertigstellen**.

Wenn der Assistent abgeschlossen ist, wird eine Benutzerprogrammkategorie erstellt. Die erstellte Kategorie kann in der Kategorienliste im Arbeitsbereich des Ordners **Programmkategorien** angezeigt werden.

Wenn Sie eine Programmkategorie in eine KLC-Datei exportieren möchten, klicken Sie mit der rechten Maustaste auf den Namen der Kategorie, wählen Sie im Menü **Exportieren** aus, geben Sie im neuen Fenster den Dateinamen an und klicken Sie anschließend auf **Speichern**.

Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

Sie können ausführbare Dateien, die sich auf die Ereignisse **Anwendungsstart verboten** und **Anwendungsstart im Testbetrieb verboten** beziehen, zu einer vorhandenen, manuell ergänzten Programmkategorie oder zu einer neuen Programmkategorie hinzufügen.

Um ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu einer Programmkategorie hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Wählen Sie auf der Registerkarte **Ereignisse** die gewünschten Ereignisse aus.
4. Wählen Sie im Kontextmenü eines der gewählten Ereignisse den Punkt **Zur Kategorie hinzufügen** aus.
5. Legen Sie im sich öffnenden Fenster **Aktion mit der zum Ereignis gehörenden ausführbaren Datei** die erforderlichen Einstellungen fest:

   Wählen Sie eine der folgenden Optionen:

   - **Zu neuer Programmkategorie hinzufügen**

     Wählen Sie diese Option aus, wenn Sie eine neue Programmkategorie erstellen möchten.

     Klicken Sie auf die Schaltfläche **Ok**, um den Assistenten für das Erstellen einer Kategorie zu starten. Als Ergebnis der Ausführung des Assistenten wird eine Kategorie mit den angegebenen Einstellungen erstellt.

     Diese Variante ist standardmäßig nicht ausgewählt.

   - **Zu bestehender Programmkategorie hinzufügen**

     Wählen Sie diese Variante, wenn in einer bestehenden Programmkategorie die Regeln ergänzt werden müssen. Wählen Sie die gewünschte Kategorie in der Liste der Programmkategorien aus.

     Diese Variante ist standardmäßig festgelegt.

   Wählen Sie im Block **Regeltyp** die Einstellungen aus:

   - **Zur Kategorie hinzufügen**

     Wählen Sie diese Variante, wenn die Regeln zu den Bedingungen einer Programmkategorie hinzugefügt werden müssen.

     Diese Variante ist standardmäßig festgelegt.

   - **Regeln zum Hinzufügen zu den Ausschlüssen**

     Wählen Sie diese Option aus, wenn Sie Regeln zu den Ausnahmen der Programmkategorie hinzufügen möchten.

   Wählen Sie im Block **Typ der Dateiinformationen** eine der Einstellungen:

   - **Zertifikatsdetails (oder SHA256-Hashes für Dateien ohne Zertifikat)**

     Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen einer Anwendung von einem Zertifikat signiert sein oder mehrere verschiedene Anwendungen eines Herstellers können von einem Zertifikat signiert sein. Bei der Wahl des Zertifikates können mehrere Anwendungsversionen oder mehrere Anwendungen eines Herstellers in der Kategorie vorhanden sein.

     Jede Datei hat ihre eindeutige SHA256-Hash-Funktion. Bei der Auswahl der SHA256-Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Anwendungsversion.

     Wählen Sie diese Variante, wenn Sie die die Zertifikatsdetails einer ausführbaren Datei (oder die SHA256-Hash-Funktion für Dateien ohne Zertifikat) zu den Regeln der Kategorie hinzufügen möchten.

     Diese Variante ist standardmäßig ausgewählt.

- **Zertifikatsdetails (Dateien ohne Zertifikat werden übersprungen)**

  Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen einer Anwendung von einem Zertifikat signiert sein oder mehrere verschiedene Anwendungen eines Herstellers können von einem Zertifikat signiert sein. Bei der Wahl des Zertifikates können mehrere Programmversionen oder mehrere Programme eines Herstellers in der Kategorie vorhanden sein.

  Wählen Sie diese Variante, wenn Sie die Zertifikatsdaten einer ausführbaren Datei zu den Regeln der Kategorie hinzufügen möchten. Wenn die ausführbare Datei kein Zertifikat hat, wird eine solche Datei übersprungen. Die entsprechenden Informationen werden nicht zur Kategorie hinzugefügt.

- **Nur SHA256 (Dateien ohne Hash werden übersprungen)**

  Jede Datei hat ihre eindeutige SHA256-Hash-Funktion. Bei der Auswahl der SHA256-Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Programmversion.

  Wählen Sie diese Variante, wenn Sie nur die Daten der SHA256-Hash-Funktion einer ausführbaren Datei hinzufügen möchten.

- **Nur MD5 (ausgelaufener Modus, nur für Version Kaspersky Endpoint Security 10 Service Pack 1)**

  Jede Datei hat ihre eindeutige MD5-Hash-Funktion. Bei der Auswahl der MD5 Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Anwendungsversion.

  Wählen Sie diese Variante, wenn Sie nur die Details der MD5-Hash-Funktion einer ausführbaren Datei hinzufügen möchten. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 1 für Windows unterstützt.

6. Klicken Sie auf die Schaltfläche **OK**.

Verwaltung des Programmstarts auf Client-Geräten anpassen

Anhand der Programmklassifizierung lässt sich die Verwaltung des Programmstarts auf Geräten optimieren. Sie können eine Programmkategorie erstellen und die Komponente Programmkontrolle der Richtlinie so anpassen, dass auf den Geräten, auf denen diese Richtlinie angewendet wird, nur Programme aus der angegebenen Kategorie gestartet werden. Zum Beispiel haben Sie die Kategorie erstellt, in der die Programme *Programm_1* und *Programm_2* enthalten sind. Nach dem Hinzufügen dieser Kategorie zur Richtlinie wird auf Geräten, auf denen diese Richtlinie angewendet wird, nur der Start von zwei Programmen, *Programm_1* und *Programm_2* erlaubt. Wenn der Benutzer versucht, ein Programm zu starten, das nicht in der Kategorie enthalten ist, beispielsweise *Program_3*, so wird der Start dieses Programms blockiert. Dem Benutzer wird eine Nachricht angezeigt sein, dass der Start von *Programm_3* gemäß den Regeln der Programmkontrolle untersagt ist. Sie können eine Kategorie erstellen, die anhand verschiedener Kriterien, die zum angegebenen Ordner gehören, automatisch ergänzt wird. In diesem Fall werden Dateien aus dem angegebenen Ordner automatisch zur Kategorie hinzugefügt. Die ausführbaren Dateien des Programms werden in den angegebenen Ordner kopiert, automatisch bearbeitet, und ihre Metriken werden in die Kategorie eingetragen.

Um die Verwaltung des Programmstarts auf Client-Geräten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Programmkategorien** aus.

2. Erstellen Sie im Arbeitsbereich des Ordners **Programmkategorien** eine Kategorie der Programme, die Sie verwalten möchten, während sie gestartet werden.

3. Klicken Sie zum Erstellen einer neuen Richtlinie für Kaspersky Endpoint Security für Windows im Ordner **Verwaltete Geräte** auf der Registerkarte **Richtlinien** auf den Link **Neue Richtlinie** und folgen Sie den Anweisungen des Assistenten.

   Ist diese Richtlinie bereits vorhanden, können Sie diesen Schritt überspringen. Die Verwaltung des Starts von Programmen der gewählten Kategorie können Sie in den Einstellungen dieser Richtlinie anpassen. Die erstellte Richtlinie wird im Ordner **Verwaltete Geräte** auf der Registerkarte **Richtlinien** angezeigt.

4. Klicken Sie mit der rechten Maustaste auf die Richtlinie für das Programm Kaspersky Endpoint Security für Windows und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Richtlinie für Kaspersky Endpoint Security für Windows geöffnet.

5. Aktivieren Sie im Eigenschaftenfenster der Richtlinie für Kaspersky Endpoint Security für Windows unter **Sicherheitskontrolle → Programmkontrolle** das Kontrollkästchen **Programmkontrolle**.

6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Regel der Programmkontrolle** wird geöffnet.

7. Wählen Sie im Fenster **Regel der Programmkontrolle** in der Dropdown-Liste **Kategorie** die Programmkategorie aus, für welche die Regel gelten soll. Passen Sie die Einstellungen der Regel für den Start von Programmen der gewählten Programmkategorien an.

   Für die Programmversionen von Kaspersky Endpoint Security 10 Service Pack 2 und höher werden Kategorien, die nach dem Kriterium MD5-Hash der ausführbaren Datei erstellt wurden, nicht angezeigt.

   Es wird nicht empfohlen, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA256-Hash einer ausführbaren Datei" erstellt wurde. Das kann zum Absturz des Programms führen.

   Ausführliche Anweisungen zur Konfiguration der Kontrollregeln finden Sie in der Online-Hilfe für Kaspersky Endpoint Security für Windows.

8. Klicken Sie auf die Schaltfläche **OK**.

Die Programme, die zur angegebenen Kategorie gehören, werden auf den Geräten nach der angegebenen Regel gestartet. Die neu erstellte Regel wird im Eigenschaftenfenster der Richtlinie für Kaspersky Endpoint Security für Windows für Windows im Abschnitt **Programmkontrolle** angezeigt.

Ergebnisse der statischen Analyse der Regeln für den Start ausführbarer Dateien anzeigen

Gehen Sie wie folgt vor, um sich Informationen darüber anzeigen zu lassen, welche ausführbaren Dateien für den Start von Benutzern nicht zugelassen sind:

1. Wählen Sie im Ordner **Verwaltete Geräte** der Konsolenstruktur die Registerkarte **Richtlinien** aus.

2. Klicken Sie mit der rechten Maustaste auf die Richtlinie für das Programm Kaspersky Endpoint Security für Windows und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster der Richtlinie der Anwendung wird geöffnet.

3. Wählen Sie im Bereich **Abschnitte** den Punkt **Sicherheitskontrolle** und dann den Unterabschnitt **Programmkontrolle**.

4. Klicken Sie auf die Schaltfläche **Statische Analyse**.

   Das Fenster **Analyse der Liste der Zugriffsrechte** wird geöffnet. Im linken Teil des Fensters wird eine Liste mit Benutzern angezeigt, die sich aus den Daten des Active Directory zusammensetzt.

5. Wählen Sie in der Liste einen Benutzer aus.

   Im rechten Fensterbereich werden Programmkategorien angezeigt, die diesem Benutzer zugewiesen wurden.

6. Um sich ausführbare Dateien anzeigen zu lassen, deren Start für den Benutzer verboten ist, klicken Sie im Fenster **Analyse der Liste der Zugriffsrechte** auf die Schaltfläche **Dateien anzeigen**.

   Daraufhin wird das Fenster geöffnet, in dem die Liste der ausführbaren Dateien angezeigt wird, deren Start für den Benutzer verboten ist.

7. Um sich die Liste der ausführbaren Dateien anzeigen zu lassen, die zu einer Kategorie gehören, wählen Sie die gewünschte Programmkategorie aus, und klicken Sie auf die Schaltfläche **Kategoriedateien anzeigen**.

   Ein Fenster wird geöffnet, in dem die Liste der ausführbaren Dateien angezeigt wird, die zur gewählten Programmkategorie gehören.

Programm-Registry anzeigen

Kaspersky Security Center führt eine Inventarisierung der Software durch, die auf den verwalteten Geräten installiert ist.

Der Administrationsagent erstellt eine Liste der auf dem Windows- oder Linux-Gerät installierten Programme und leitet die Liste an den Administrationsserver weiter. Bei Windows-basierten Client-Geräten erhält der Administrationsagent die meisten Informationen über installierte Programme aus der Windows-Registrierung. Bei Linux-basierten Client-Geräten werden dem Administrationsagenten die Informationen über installierte Programme durch die Paketmanager bereitgestellt.

Um sich die Registry der auf den Client-Geräten installierten Programme anzeigen zu lassen,

Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Programm-Registry** aus.

Im Arbeitsbereich des Ordners **Programm-Registry** wird dann eine Liste mit Programmen angezeigt, die auf den Client-Geräten und dem Administrationsserver installiert sind.

Detaillierte Informationen über ein bestimmtes Programm aus der Liste können Sie über den Punkt **Eigenschaften** im Kontextmenü dieses Programms anzeigen lassen. Im Eigenschaftenfenster des Programms werden allgemeine Informationen zum Programm und dessen ausführbaren Dateien sowie die Liste der Geräte angezeigt, auf denen das Programm installiert wurde.

Im Kontextmenü jedes Programms in der Liste sind folgende Aktionen verfügbar:

- Programm zu einer Programmkategorie hinzufügen.
- Dem Programm ein Tag zuweisen.
- Liste der Programme als csv- oder txt-Datei exportieren.
- Programmeigenschaften anzeigen, z. B. Name des Anbieters, Versionsnummer, Liste der ausführbaren Dateien, Liste mit Geräten, auf denen das Programm installiert ist, Liste mit verfügbaren Programm-Updates oder Liste mit gefundenen Schwachstellen in Programmen.

Um sich Programme anzeigen zu lassen, die bestimmten Kriterien entsprechen, können Sie die Filterfelder im Arbeitsbereich des Ordners **Programm-Registry** verwenden.

Im Eigenschaftenfenster des ausgewählten Gerätes können Sie im Abschnitt **Programm-Registry** eine Liste der Programme anzeigen, die auf dem Gerät installiert sind.

Bericht über installierte Programme generieren

Sie können außerdem im Arbeitsbereich der **Programm-Registry** auf die Schaltfläche **Bericht über installierte Programme anzeigen** klicken, um einen Bericht zu erstellen, der eine detaillierte Statistik zu den installierten Programmen enthält und angibt, auf wie vielen Geräten das jeweilige Programm installiert ist. Dieser Bericht, der auf der Seite **Bericht über installierte Programme** geöffnet wird, enthält Informationen über sowohl Kaspersky-Anwendungen als auch Drittanbieter-Programme. Wenn Sie nur Informationen zu Kaspersky-Anwendungen sehen möchten, die auf Client-Geräten installiert sind, wählen Sie in der Liste **Zusammenfassung** den Punkt "AO Kaspersky Lab".

Die Daten über Kaspersky-Anwendungen und Drittanbieter-Programmen auf den Geräten, die mit sekundären und virtuellen Administrationsservern verbunden sind, werden auch in der Programm-Registry des primären Administrationsservers gespeichert. Nachdem Sie die Daten der sekundären und virtuellen Administrationsserver hinzugefügt haben, klicken Sie auf die Schaltfläche **Bericht über installierte Programme anzeigen**. Auf der folgenden Seite **Bericht über installierte Programme** können Sie diese Informationen einsehen.

Um Informationen von sekundären und virtuellen Administrationsservern in den Bericht über installierte Programme aufzunehmen:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie auf der Registerkarte **Berichte** die Option **Bericht über installierte Programme**.
4. Klicken Sie mit der rechten Maustaste auf den Bericht und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Fenster der **Eigenschaft: Bericht über installierte Programme** geöffnet.
5. Aktivieren Sie im Abschnitt **Hierarchie der Administrationsserver** das Kontrollkästchen **Daten von sekundären und virtuellen Administrationsservern einschließen**.
6. Klicken Sie auf die Schaltfläche **OK**.

   Daraufhin werden Informationen über die sekundären und virtuellen Administrationsserver in den Bericht **Bericht über installierte Programme** aufgenommen.

Startzeit der Software-Inventur ändern

Kaspersky Security Center führt eine Inventarisierung der Software durch, die auf den verwalteten Client-Geräten unter Windows installiert ist.

Der Administrationsagent erstellt eine Liste der auf dem Gerät installierten Programme und leitet die Liste an den Administrationsserver weiter. Der Administrationsagent erhält Informationen über die installierten Programme automatisch aus der Windows-Registry.

Um die Ressourcen des Geräts zu speichern beginnt der Administrationsagent standardmäßig 10 Minuten nach dem Start des Dienstes des Administrationsagenten, Informationen über die installierten Programme abzurufen.

Um die Zeitspanne für den Beginn der Softwareinventarisierung des Geräts nach dem Start des Dienstes des Administrationsagenten zu ändern, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsagent installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** → **Ausführen**.

2. Rufen Sie den folgenden Abschnitt auf:

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags

   - Für 64-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF

3. Legen Sie für den Schlüssel KLINV_INV_COLLECTOR_START_DELAY_SEC den gewünschten Wert in Sekunden fest.

   Standardmäßig ist der Wert auf 600 Sekunden eingestellt.

4. Starten Sie den Dienst des Administrationsagenten neu.

Daraufhin wird die Zeitspanne für den Beginn der Software-Inventur nach dem Start des Dienstes des Administrationsagenten geändert.

Über die Verwaltung von Lizenzschlüsseln von Drittanbieter-Programmen

Mit Kaspersky Security Center können Sie Nutzung von Lizenzschlüsseln der auf verwalteten Geräten installierten Drittanbieter-Programme überwachen. Die Liste mit den Programmen, deren Lizenzschlüsselnutzung Sie überwachen können, wird der Programm-Registry entnommen. Für jeden Lizenzschlüssel können Sie die Verletzungen für die folgenden Beschränkungen konfigurieren und überwachen:

- Maximale Anzahl der Geräte, auf denen das Programm installiert werden darf, das diesen Lizenzschlüssel verwendet
- Ablaufdatum des Lizenzschlüssels

Kaspersky Security Center prüft nicht, ob der angegebene Lizenzschlüssel gültig ist oder nicht. Sie können nur Beschränkungen überwachen, die Sie konfiguriert haben. Wenn eine der Beschränkungen, die Sie einem Lizenzschlüssel auferlegen, verletzt wird, registriert der Administrationsserver ein Ereignis des Typs Information, Warnung oder Funktionsfehler.

Lizenzschlüssel sind an Programmgruppen gebunden. Eine Programmgruppe ist eine Gruppe von Drittanbieter-Programmen, die Sie auf Grundlage verschiedener Kriterien zusammenstellen. Sie können Programme über den Namen eines Programms, über seine Version, seinen Hersteller und sein Tag definieren. Ein Programm wird dann der Gruppe hinzugefügt, wenn mindestens eins der Kriterien erfüllt ist. Jede Programmgruppe kann mehrere Lizenzschlüssel binden, aber jeder Lizenzschlüssel ist an eine einzige Programmgruppe gebunden.

Ein weiteres Werkzeug zum Überwachen der Lizenzschlüsselnutzung ist der Bericht über den Status lizenzierter Programmgruppen. Dieser Bericht enthält Informationen über den aktuellen Status der lizenzierten Programmgruppen, einschließlich:

- Anzahl der Installationen von Lizenzschlüsseln für jede Programmgruppe
- Anzahl der benutzten und unbenutzten Lizenzschlüssel
- Detaillierte Liste der Anwendungen, die auf verwalteten Geräten installiert sind

Die Werkzeuge zur Verwaltung von Lizenzschlüsseln von Drittanbieter-Programmen befinden sich im Unterordner **Verwendung von Drittanbieter-Lizenzen** (**Erweitert** → **Programmverwaltung** → **Verwendung von Drittanbieter-Lizenzen**). In diesem Unterordner können Sie Programmgruppen erstellen, Lizenzschlüssel hinzufügen und den Bericht über den Status lizenzierter Programmgruppen generieren.

Die Tools zur Lizenzschlüsselverwaltung von Drittanbieteranwendungen sind nur verfügbar, wenn Sie im Fenster **Benutzeroberfläche konfigurieren** die Option "Schwachstellen- und Patch-Management" aktiviert haben.

Lizenzierte Programmgruppen erstellen

Um eine lizenzierte Programmgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Verwendung von Drittanbieter-Lizenzen** aus.
2. Klicken Sie auf die Schaltfläche **Lizenzierte Programmgruppe hinzufügen**, um den Assistent für das Hinzufügen einer Gruppe lizenzierter Programme auszuführen.

   Der Assistent für das Hinzufügen einer Gruppe lizenzierter Programme wird gestartet.
3. Geben Sie im Schritt **Informationen zur lizenzierten Programmgruppe** die Programme an, die in der Programmgruppe enthalten sein sollen:

   - **Name der lizenzierten Programmgruppe**
   - **Lizenzverletzung protokollieren**

     Wenn eine der Beschränkungen, die Sie einem Lizenzschlüssel auferlegen, verletzt wird, registriert der Administrationsserver ein Ereignis des Typs Information, Warnung oder Funktionsfehler:

     - Ereignistyp "Information": **Die Beschränkung für die Anzahl von Installationen wird für eine der lizenzierten Programmgruppen bald überschritten (mehr als 95% verbraucht)**
     - Ereignistyp "Warnung": **Für eine der lizenzierten Programmgruppen wird die Beschränkung für die Anzahl von Installationen bald überschritten**
     - Ereignistyp "Funktionsfehler": **Für eine der lizenzierten Programmgruppen wurde die Beschränkung für die Anzahl von Installationen überschritten**

       Ein Ereignis wird nur einmal ausgelöst – und zwar wenn die angegebene Bedingung erfüllt wird. Das Ereignis kann erst dann erneut ausgelöst werden, wenn die Anzahl der Installationen auf ein normales Level zurückgegangen ist und das Ereignis anschließend wiederholt eintritt. Ein Ereignis kann maximal einmal pro Stunde ausgelöst werden.

- **Kriterien für die Aufnahme von gefundenen Programmen in diese lizenzierte Programmgruppe**

  Geben Sie Kriterien an, die definieren, welche Programme in der Programmgruppe enthalten sein soll. Sie können Programme über den Namen eines Programms, über seine Version, seinen Hersteller und sein Tag definieren. Es muss mindestens ein Kriterium angegeben werden. Ein Programm wird dann der Gruppe hinzugefügt, wenn mindestens eins der Kriterien erfüllt ist.

4. Geben Sie im Schritt **Geben Sie Daten zu den vorhandenen Lizenzschlüsseln ein** die Lizenzschlüssel an, den Sie überwachen möchten. Wählen Sie die Option **Verstoß gegen die festgelegten Lizenzbeschränkungen protokollieren** und fügen Sie anschließend die Lizenzschlüssel hinzu:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   b. Wählen Sie den hinzuzufügenden Lizenzschlüssel aus und klicken Sie auf **OK**. Wenn der benötigte Lizenzschlüssel nicht aufgelistet wird, klicken Sie auf **Hinzufügen** und geben Sie anschließend die Eigenschaften des Lizenzschlüssels an.

5. Klicken Sie im Schritt **Lizenzierte Programmgruppe hinzufügen** auf die Schaltfläche **Fertigstellen**.

Es wird eine lizenzierte Programmgruppe erstellt, die im Ordner **Lizenzverwaltung für Verwendung von Drittanbieter-Lizenzen** angezeigt wird.

Verwaltung von Lizenzschlüsseln für lizenzierte Programmgruppen

Um einen Lizenzschlüssel für eine lizenzierte Programmgruppe zu erstellen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Verwendung von Drittanbieter-Lizenzen** aus.

2. Klicken Sie im Arbeitsbereich des Ordners **Verwendung von Drittanbieter-Lizenzen** auf die Schaltfläche **Lizenzschlüssel für lizenzierte Programme verwalten**.

   Das Fenster **Lizenzschlüsselverwaltung in lizenzierten Programmen** wird geöffnet.

3. Klicken Sie im Fenster **Lizenzschlüsselverwaltung in lizenzierten Programmen** auf **Hinzufügen**.

   Das Fenster **Lizenzschlüssel** wird geöffnet.

4. Geben Sie im Fenster **Lizenzschlüssel** die Eigenschaften des Lizenzschlüssels an und die Beschränkungen des Lizenzschlüssels für die lizenzierte Programmgruppe.

   - **Name**. Name des Lizenzschlüssels.
   - **Kommentar**. Anmerkungen zum ausgewählten Lizenzschlüssel.
   - **Beschränkung**. Anzahl der Geräte, auf denen das Programm installiert werden darf, das diesen Lizenzschlüssel verwendet.
   - **Gültig bis**. Ablaufdatum des Lizenzschlüssels.

Erstellte Lizenzschlüssel werden im Fenster **Lizenzschlüsselverwaltung in lizenzierten Programmen** angezeigt.

Um einen Lizenzschlüssel auf eine lizenzierte Programmgruppe anzuwenden:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Verwendung von Drittanbieter-Lizenzen** aus.
2. Wählen Sie im Ordner **Verwendung von Drittanbieter-Lizenzen** die lizenzierte Programmgruppe aus, auf die Sie einen Lizenzschlüssel anwenden möchten.
3. Klicken Sie mit der rechten Maustaste auf die lizenzierte Programmgruppe und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der lizenzierten Programmgruppe geöffnet.
4. Wählen Sie im Eigenschaftenfenster der lizenzierten Programmgruppe im Abschnitt **Lizenzschlüssel** die Option **Verstoß gegen die festgelegten Lizenzbeschränkungen protokollieren** aus.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Lizenzschlüssel auswählen** wird geöffnet.
6. Wählen Sie im Fenster **Lizenzschlüssel auswählen** den Lizenzschlüssel aus, den Sie auf die lizenzierte Programmgruppe anwenden möchten.
7. Klicken Sie auf die Schaltfläche **OK**.

Beschränkungen, die für eine lizenzierte Programmgruppe gelten und im Lizenzschlüssel angegeben sind, werden auch auf die ausgewählte lizenzierte Programmgruppe angewendet.

Inventarisierung der ausführbaren Dateien

Sie können eine Liste der auf verwalteten Geräten gespeicherten ausführbaren Dateien abrufen. Um ausführbare Dateien zu inventarisieren, müssen Sie eine Inventarisierungsaufgabe erstellen.

Die Funktion zum Inventarisieren ausführbarer Dateien ist für die folgenden Programme verfügbar:

- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization 4.0 Light Agent und höhere Versionen

Die Anzahl ausführbarer Dateien, die von einem Gerät erhalten werden, darf 150.000 nicht überschreiten. Wenn diese Beschränkung erreicht ist, kann Kaspersky Security Center keinen neuen Daten mehr empfangen.

Bevor Sie beginnen, aktivieren Sie die Benachrichtigungen über den Start von Programmen in den Richtlinien von Kaspersky Endpoint Security und des Administrationsagenten, damit Sie Daten auf den Administrationsserver übertragen können.

So aktivieren Sie die Benachrichtigungen über den Start von Programmen:

- Öffnen Sie die Richtlinieneinstellungen von Kaspersky Endpoint Security und gehen Sie wie folgt vor:

  1. Wechseln Sie zu **Allgemeine Einstellungen → Berichte und Speicherung**.
  2. Aktivieren Sie im Abschnitt **Datenübertragung zum Administrationsserver** das Kontrollkästchen **Über gestartete Anwendungen**.
  3. Speichern Sie Ihre Änderungen.

- Öffnen Sie die Richtlinieneinstellungen des Administrationsagenten und gehen Sie wie folgt vor:

  1. Wechseln Sie zum Abschnitt **Datenverwaltung**.
  2. Aktivieren Sie das Kontrollkästchen **Details zu installierten Programmen**.
  3. Speichern Sie Ihre Änderungen.

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Klicken Sie im Arbeitsbereich des Ordners **Aufgaben** auf die Schaltfläche **Neue Aufgabe**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten den Aufgabentyp **Kaspersky Endpoint Security** und den Aufgabentyp **Inventarisierung**. Klicken Sie auf die Schaltfläche **Weiter**.
4. Folgen Sie den weiteren Schritten des Assistenten.

   Nach der Ausführung des Assistenten wird eine Inventarisierungsaufgabe für Kaspersky Endpoint Security erstellt. Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsbereich des Ordners **Aufgaben** angezeigt.

Eine Liste der auf den Geräten als Ergebnis der Ausführung der Inventarisierungsaufgaben gefundenen ausführbaren Dateien wird im Arbeitsbereich des Ordners **Ausführbare Dateien** angezeigt.

Während der Inventarisierung findet das Programm ausführbare Dateien folgender Formate: mz, com, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, sowie HTML-Dateien.

Informationen über ausführbare Dateien anzeigen

Um sich die Liste aller auf den Client-Geräten gefundenen ausführbaren Dateien anzeigen zu lassen,

Wählen Sie im Ordner **Programmverwaltung** der Konsolenstruktur den Unterordner **Ausführbare Dateien** aus.

Im Arbeitsbereich des Ordners **Ausführbare Dateien** wird die Liste mit ausführbaren Dateien angezeigt, die entweder auf den Geräten ausgeführt wurden oder während der Ausführung der Inventarisierungsaufgabe von Kaspersky Endpoint Security für Windows gefunden wurden.

Um sich die Daten zu den ausführbaren Dateien anzeigen zu lassen, die bestimmten Kriterien entsprechen, können Sie den Filter verwenden.

Um sich die Eigenschaften einer ausführbaren Datei anzeigen zu lassen,

klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Eigenschaften** aus.

Daraufhin wird das Fenster geöffnet, in dem Informationen über die ausführbare Datei sowie Geräte angezeigt werden, auf denen die ausführbare Datei vorhanden ist.

Überwachung und Berichterstattung

In diesem Abschnitt werden die Möglichkeiten für die Überwachung und die Berichterstellung von Kaspersky Security Center beschrieben. Diese Möglichkeiten geben Ihnen einen Überblick über Ihre Infrastruktur, die Schutzstatus und Statistiken.

Nach der Bereitstellung von Kaspersky Security Center oder während des Programmbetriebs können Sie die Funktionen für die Überwachung und für die Berichterstellung an Ihre Bedürfnisse anpassen.

- **Farbliche Kennzeichnung**

  Mithilfe der farblichen Kennzeichnungen kann der aktuelle Status von Kaspersky Security Center und der verwalteten Geräte in der Verwaltungskonsole rasch bewertet werden.

- **Statistik**

  Statistische Informationen über den Status des Schutzsystems und der verwalteten Geräte werden als anpassbare Informationsbereiche dargestellt.

- **Berichte**

  Mithilfe von Berichten können Sie detaillierte, zahlenbasierte Informationen zur Sicherheit Ihres Unternehmensnetzwerkes zusammenstellen und diese Informationen in einer Datei speichern, per E-Mail versenden und ausdrucken.

- **Ereignisse**

  Die Ereignisauswahlen bieten eine Bildschirmansicht der benannten Ereignisgruppen, die aus der Administrationsserver-Datenbank ausgewählt wurden. Diese Sätze von Ereignissen sind nach den folgenden Kategorien gruppiert:

  - Nach Ereigniskategorie – **Kritische Ereignisse**, **Funktionsfehler**, **Warnungen** und **Informative Ereignisse**
  - Nach Zeit – **Letzte Ereignisse**
  - Nach Typ – **Benutzeranfragen** und **Audit-Ereignisse**

Benutzerdefinierte Ereignisauswahlen können Sie auf der Basis von Einstellungen, die in der Oberfläche von Kaspersky Security Center Web Console verfügbar sind, erstellen und anzeigen.

Szenario: Überwachung und Berichterstattung

Dieser Abschnitt enthält ein Szenario zur Konfiguration der Funktion der Überwachung und Berichterstellung in Kaspersky Security Center.

Erforderliche Vorrausetzungen

Nach der Verteilung von Kaspersky Security Center im Unternehmensnetzwerk können Sie mit seiner Überwachung beginnen und Berichte zum Netzwerkbetrieb erstellen.

Schritte

Die Überwachung und Berichterstellung in einem Unternehmensnetzwerk erfolgt in mehreren Etappen:

1. **Einstellungen zum Umschalten der Status von Geräten**

   Machen Sie sich mit den Einstellungen vertraut, die den Gerätestatus in Abhängigkeit von bestimmten Bedingungen vorgeben. Wenn Sie diese Einstellungen anpassen, können Sie auch die Anzahl der Ereignisse der Ereigniskategorie *Kritisch* oder *Warnung* ändern.

   Stellen Sie bei der Konfigurieren des Wechsels des Gerätestatus sicher, dass die neuen Einstellungen nicht mit den Richtlinien zur Informationssicherheit Ihres Unternehmens in Konflikt stehen und dass Sie rechtzeitig auf wichtige Sicherheitsereignisse im Netzwerk Ihres Unternehmens reagieren können.

2. **Einstellungen für Benachrichtigungen über Ereignisse auf Client-Geräten anpassen**

   Passen Sie die Benachrichtigungen (per E-Mail, SMS oder durch Start einer ausführbaren Datei) zu Ereignissen auf Client-Geräten entsprechend den Bedürfnissen Ihres Unternehmens an.

3. **Ändern Sie die Reaktion Ihres Sicherheitsnetzwerks auf das Virenangriff-Ereignis**

   Um die Reaktion des Netzwerks auf neue Ereignisse anzupassen, können Sie in den Eigenschaften des Administrationsservers die spezifischen Schwellenwerte ändern. Sie können außerdem eine strengere Richtlinie erstellen, die in einem solchen Fall aktiviert wird, oder eine Aufgabe erstellen, die bei Auftreten dieses Ereignisses ausgeführt wird.

4. **Arbeiten mit statistischen Daten**

   Konfigurieren Sie die Anzeige von Statistiken entsprechend den Bedürfnissen Ihrer Organisation.

5. **Sicherheitsstatus Ihres Unternehmensnetzwerks verfolgen**

   Sie können einen der folgenden Schritte ausführen, um den Sicherheitsstatus Ihres Unternehmensnetzwerks zu überprüfen:

   - Öffnen Sie im Arbeitsbereiche des Knotens **Administrationsserver**, auf der Registerkarte **Statistik** die zweite Ebene (Seite) **Schutzstatus** und prüfen Sie den Informationsbereich **Status des Echtzeitschutzes**
   - **Bericht über den Schutzstatus** erstellen und überprüfen
   - **Fehlerbericht** erstellen und überprüfen

6. **Client-Geräte finden, die nicht geschützt sind**

   Um ungeschützte Client-Geräte zu finden, wechseln Sie in den Arbeitsbereich des Knotens **Administrationsserver**, öffnen Sie auf der Registerkarte **Statistik** die zweite Ebene (Seite) **Schutzstatus** und prüfen Sie den Informationsbereich **Verlauf der im Netzwerk gefundenen neuen Geräte**. Sie können auch den **Bericht über die Bereitstellung des Schutzes** erzeugen und überprüfen.

7. **Schutz der Client-Geräte überprüfen**

   Um den Schutzstatus von Client-Geräten zu überprüfen, wechseln Sie in den Arbeitsbereich des Knotens **Administrationsserver**, und öffnen Sie auf der Registerkarte **Statistik** die zweite Ebene (Seite) **Bereitstellung** oder **Bedrohungsstatistiken**. Prüfen Sie die relevanten Informationsbereiche. Sie können außerdem die Ereignisauswahl **Kritische Ereignisse** starten und überprüfen.

8. **Ereignismenge für Datenbank einschätzen und einschränken**

   Informationen über Ereignisse im Betrieb der verwalteten Anwendungen werden vom Client-Gerät übertragen und in der Administrationsserver-Datenbank registriert. Um die Belastung auf den Administrationsserver zu reduzieren, sollten Sie die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, einschätzen und einschränken.

   Um die Auslastung der Datenbank durch Ereignisse zu bewerten, berechnen Sie den Speicherplatz der Datenbank. Sie können auch die maximale Anzahl von Ereignissen begrenzen um einen Datenbanküberlauf zu vermeiden.

9. **Lizenzinformationen überprüfen**

   Um Lizenzinformationen zu prüfen, wechseln sie in den Arbeitsbereich des Knotens **Administrationsserver**, öffnen Sie auf der Registerkarte **Statistik** die zweite Ebene (Seite) **Bereitstellung** und prüfen Sie den Informationsbereich **Nutzung von Lizenzschlüsseln**. Sie können auch den **Bericht über die Lizenzschlüsselnutzung** erzeugen und überprüfen.

Ergebnisse

Nach Abschluss des Szenarios werden Sie über den Schutz Ihres Unternehmensnetzwerks informiert und können Aktionen für den weiteren Schutz des Netzwerks planen.

Farbliche Kennzeichnungen und protokollierte Ereignissen in der Verwaltungskonsole überwachen

Mithilfe der farblichen Kennzeichnungen kann der aktuelle Status von Kaspersky Security Center und der verwalteten Geräte in der Verwaltungskonsole rasch bewertet werden. Die Kennzeichnungen werden im Arbeitsbereich des Knotens **Administrationsserver** auf der Registerkarte **Überwachung** angezeigt. Auf der Registerkarte gibt es sechs Informationsbereiche mit farblichen Kennzeichnungen und protokollierten Ereignissen. Die farbliche Kennzeichnung besteht aus einer farbigen vertikalen Leiste auf der linken Seite des Bereichs. Jeder Block mit Kennzeichnung steht für einen separaten funktionalen Bereich von Kaspersky Security Center (s. Tabelle unten).

Zuständigkeitsbereiche der farblichen Kennzeichnungen in der Verwaltungskonsole

Bereichsname	Zuständigkeitsbereich der farblichen Kennzeichnung
Bereitstellung	Installation des Administrationsagenten und der Sicherheitsanwendungen auf den Geräten im Unternehmensnetzwerk
Verwaltungsstruktur	Struktur der Administrationsgruppen. Scannen des Netzwerkes. Verschiebungsregeln für Geräte
Schutzeinstellungen	Funktionen der Sicherheitsanwendung: Schutzstatus, Schadsoftware-Untersuchung
Update	Updates und Patches

Bereichsname	Zuständigkeitsbereich der farblichen Kennzeichnung
Überwachung	Schutzstatus
Administrationsserver	Funktionen und Eigenschaften des Administrationsservers

Die Kennzeichnung kann eine von fünf Farben aufweisen (s. Tabelle unten). Die Farbe der Kennzeichnung hängt vom aktuellen Status von Kaspersky Security Center und den registrierten Ereignissen ab.

Farbkodierung der Kennzeichnungen

Status	Farbe der Kennzeichnung	Farbwert der Kennzeichnung
Informativ	Grün	Keine Aktion des Administrators erforderlich.
Warnung	Gelb	Es ist eine Aktion des Administrators erforderlich.
Kritisch	Rot	Es gibt ernste Probleme. Für deren Behebung ist eine Aktion des Administrators erforderlich.
Informativ	Blau	Es sind Ereignisse registriert, die nicht mit potentiellen oder tatsächlichen Bedrohungen für die Sicherheit der verwalteten Geräte verbunden sind.
Informativ	Grau	Keine Informationen über die Ereignisse verfügbar oder noch keine Informationen erhalten.

Der Administrator sollte dafür sorgen, dass die Farbkennzeichnung aller Informationsbereiche auf der Registerkarte **Überwachung** grün bleibt.

In den Informationsbereichen werden auch protokollierte Ereignisse angezeigt, die sich auf die Farbkennzeichnungen und den Status von Kaspersky Security Center auswirken (siehe Tabelle unten).

Name, Beschreibung und farbliche Kennzeichnung der protokollierten Ereignisse

Farbe der Kennzeichnung	Dargestellter Name des Ereignistyps	Ereignistyp	Beschreibung
Rot	**Lizenz ist auf %1 Gerät(en) abgelaufen**	IDS_AK_STATUS_LIC_EXPAIRED	Ereignisse dieser Art treten auf, wenn der Gültigkeitszeitraum einer kommerziellen Lizenz abgelaufen ist. Kaspersky Security Center prüft einmal täglich, ob die Lizenz auf den Geräten abgelaufen ist. Wenn die kommerzielle Lizenz abläuft, stellt Kaspersky Security Center nur grundlegende Funktionen bereit. Um Kaspersky Security Center weiter Verwenden zu können, müssen Sie die kommerziellen Lizenz verlängern.
Rot	**Die Sicherheitsanwendung wurde nicht gestartet auf: %1 Gerät(en)**	IDS_AK_STATUS_AV_NOT_RUNNING	Ereignisse dieser Art treten auf, wenn die auf dem Gerät installierte Sicherheitsanwendung nicht ausgeführt wird. Stellen Sie sicher, dass Kaspersky Endpoint Security auf dem Gerät ausgeführt wird.
Rot	**Schutz nicht gestartet auf: %1 Gerät(en)**	IDS_AK_STATUS_RTP_NOT_RUNNING	Ereignisse dieser Art treten auf, wenn die Sicherheitsanwendung auf dem Gerät länger deaktiviert war, als per festgelegtem Zeitintervall erlaubt. Überprüfen Sie den aktuellen Status des Echtzeitschutzes auf dem Gerät und stellen Sie sicher, dass alle benötigten Schutzkomponenten aktiviert sind.

Farbe der Kennzeichnung	Dargestellter Name des Ereignistyps	Ereignistyp	Beschreibung
Rot	**Auf den Geräten wurde eine Schwachstelle in Programmen gefunden**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Ereignisse dieser Art treten auf, wenn die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* auf dem Gerät Schwachstellen mit der Signifikanz gefunden hat, die in den installierten Programmen auf dem Gerät angegeben wurde Prüfen Sie die Liste der verfügbaren Updates im Unterordner **Programm-Updates**, der sich im Ordner **Programmverwaltung** befindet. Dieser Ordner enthält eine Liste der durch den Administrationsserver heruntergeladenen Updates für Microsoft-Programme und Programme anderer Softwarehersteller, die auf Geräte verteilt werden können. Nachdem Sie die Informationen über die verfügbaren Updates geprüft haben, installieren Sie die Updates auf den Geräten.
Rot	**Auf dem Administrationsserver wurden kritische Ereignisse registriert**	IDS_AK_STATUS_EVENTS_OCCURED	Ereignisse dieser Art treten auf, wenn kritische Ereignisse des Administrationsservers erkannt werden. Überprüfen Sie die Liste Ereignisse, die auf dem Administrationsserver gespeichert ist, und korrigieren Sie die kritischen Ereignisse nacheinander.
Rot	**Es wurden Fehler in Ereignissen auf dem Administrationsserver protokolliert**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Ereignisse dieser Art treten auf, wenn auf der Seite des Administrationsservers unerwartete Fehler protokolliert werden. Überprüfen Sie die Liste Ereignisse, die auf dem Administrationsserver gespeichert ist, und korrigieren Sie die Fehler-Ereignisse nacheinander.
Rot	**Verbindung mit %1 Gerät(en) wurde unterbrochen**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Ereignisse dieser Art treten auf, wenn die Verbindung zwischen dem Administrationsserver und dem Gerät unterbrochen wird. Zeigen Sie die Liste mit den nicht verbundenen Geräten an und versuchen Sie, diese erneut zu verbinden.
Rot	**Der Administrationsserver hatte seit Langem keine Verbindung zu %1 Gerät(en)**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Ereignisse dieser Art treten auf, wenn sich das Gerät innerhalb des festgelegten Zeitraums nicht mit dem Administrationsserver verbunden hat, da das Gerät ausgeschaltet war. Stellen Sie sicher, dass das Gerät eingeschaltet ist und der Administrationsagent auf ihm ausgeführt wird.
Rot	**%1 Gerät(e) ohne Status OK**	IDS_AK_STATUS_HOST_NOT_OK	Ereignisse dieser Art treten auf, wenn sich der Status *OK* des mit dem Administrationsserver verbundenen Geräts in *Kritisch* oder *Warnung* ändert. Sie können das Problem mithilfe des Tools zur Ferndiagnose von Kaspersky Security Center beheben.
Rot	**Datenbanken sind veraltet auf: %1 Gerät(en)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Ereignisse dieser Art treten auf, wenn die Antiviren-Datenbanken auf dem Gerät nicht innerhalb des festgelegten Zeitraums aktualisiert wurden. Folgen Sie den Anweisungen, um die Kaspersky-Datenbanken zu aktualisieren.

Farbe der Kennzeichnung	Dargestellter Name des Ereignistyps	Ereignistyp	Beschreibung
Rot	**Gerät(e) mit lange nicht ausgeführter Suche nach Windows-Updates: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Ereignisse dieser Art treten auf, wenn die Aufgabe *Windows-Updates synchronisieren* nicht innerhalb des angegebenen Zeitintervalls ausgeführt wurde. Folgen Sie den Anweisungen, um Updates von Windows Update mit dem Administrationsserver zu synchronisieren.
Rot	**Die Installation von %1 Plug-in(s) für Kaspersky Security Center ist erforderlich**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Ereignisse dieser Art treten auf, wenn Sie zusätzliche Plug-ins für Kaspersky-Anwendungen installieren müssen. Laden Sie die erforderlichen Verwaltungs-Plug-ins für die Kaspersky-Anwendung von der Webseite des Technischen Supports von Kaspersky herunter und installieren Sie sie.

Arbeiten mit Berichten, Statistiken und Benachrichtigungen

Diesem Abschnitt können Sie Informationen über die Arbeit mit Berichten, Statistiken und Ereignis- und Geräteauswahlen in Kaspersky Security Center sowie über die Konfiguration der Administrationsserver-Benachrichtigungen entnehmen.

Arbeiten mit Berichten

Berichte in Kaspersky Security Center enthalten Informationen über den Zustand der verwalteten Geräte. Berichte werden anhand der Daten erstellt, die auf dem Administrationsserver gespeichert werden. Sie können Berichte für folgende Objekte erstellen:

- für Geräteauswahlen, die nach bestimmten Parametern erstellt wurden
- für Administrationsgruppen
- für eine Reihe von Geräten aus verschiedenen Administrationsgruppen
- für alle Geräte im Netzwerk (im Bericht über die Bereitstellung)

Das Programm verfügt über eine Auswahl von Standard-Berichtsvorlagen. Ferner gibt es die Möglichkeit zum Erstellen von benutzerdefinierten Berichtsvorlagen. Berichte werden im Programmhauptfenster im Ordner **Administrationsserver** der Konsolenstruktur angezeigt.

Berichtsvorlage erstellen

Um eine Berichtsvorlage zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Klicken Sie auf die Schaltfläche **Neue Berichtsvorlage**.

   Daraufhin wird der Assistent für das Erstellen einer Berichtsvorlage gestartet. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die erstellte Berichtsvorlage zum ausgewählten Ordner **Administrationsserver** der Konsolenstruktur hinzugefügt. Diese Vorlage kann nun zum Erstellen und Anzeigen von Berichten verwendet werden.

Eigenschaften von Berichtsvorlagen anzeigen und bearbeiten

Sie können grundlegenden Eigenschaften einer Berichtsvorlage anzeigen und ändern, beispielsweise den Namen der Berichtsvorlage oder die im Bericht angezeigten Felder.

Um die Eigenschaften einer Berichtsvorlage anzuzeigen und zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie in der Liste der Berichtsvorlagen die gewünschte Berichtsvorlage aus.
4. Wählen Sie im Kontextmenü der gewählten Berichtsvorlage **Eigenschaften** aus.

   Alternativ dazu können Sie zuerst den Bericht generieren und dann entweder auf **Eigenschaften der Berichtsvorlage öffnen** oder **Berichtsspalten anpassen** klicken.
5. Ändern Sie im angezeigten Fenster die Eigenschaften der Berichtsvorlage. Die Eigenschaften jedes Berichts dürfen nur einige der unten beschriebenen Abschnitte enthalten.

   - Abschnitt **Allgemein**:
     - Name der Berichtsvorlage
     - **Maximale Anzahl der angezeigten Einträge**

       Wenn diese Option aktiviert ist, übersteigt die Anzahl der Einträge in der Tabelle mit detaillierten Berichtsdaten den angegebene Wert nicht.

       Die Berichtseinträge werden zuerst nach den Regeln sortiert, die im Abschnitt **Felder → Detail-Felder** der Eigenschaften der Berichtsvorlage angegeben sind, und nur der erste der resultierenden Einträge wird beibehalten. Die Überschrift der Tabelle mit detaillierten Berichtsdaten zeigt die angezeigte Anzahl von Einträgen und die insgesamt verfügbare Anzahl von Einträgen, die mit anderen Berichtsvorlageneinstellungen übereinstimmen.

Wenn diese Option deaktiviert ist, zeigt die Tabelle mit detaillierten Berichtsdaten alle verfügbaren Einträge an. Es wird nicht empfohlen, diese Option zu deaktivieren. Durch die Begrenzung der Anzahl der angezeigten Berichtseinträge wird das Datenbankverwaltungssystem (DBMS) entlastet und der Zeitaufwand für das Generieren und Exportieren des Berichts verringert. Einige der Berichte enthalten zu viele Einträge. Wenn dies der Fall ist, kann es schwierig sein, sie alle zu lesen und zu analysieren. Außerdem kann es sein, dass die Erstellung eines solchen Berichts zu einer Erschöpfung der Speicherressourcen Ihres Geräts führt und Sie den Bericht dann nicht ansehen können.

Diese Option ist standardmäßig aktiviert. Als Standardwert ist 1.000 vorgegeben.

- **Druckversion**

  Die Berichtsausgabe ist für den Druck optimiert: Zur besseren Sichtbarkeit werden zwischen einigen Werten Leerzeichen eingefügt.

  Diese Option ist standardmäßig aktiviert.

- Abschnitt **Felder**.

  Wählen Sie die Felder aus, die im Bericht angezeigt werden sollen, und passen Sie an, ob die Informationen im Bericht nach jedem der Felder sortiert und gefiltert werden müssen.

- Abschnitt **Zeitintervall**.

  Ändern Sie das Zeitintervall. Die folgenden Werte sind verfügbar:

  - Zwischen den beiden angegebenen Daten
  - Vom angegebenen Datum bis zum Erstellungsdatum des Berichts
  - Vom angegebenen Datum der Berichterstellung abzüglich der Tage bis zum Erstellungsdatum des Berichts

- **Gruppe**, **Geräteauswahl** oder Abschnitt **Geräte**.

  Ändern Sie den Satz für Client-Geräte, für die der Bericht erstellt wird. Je nach den bei der Erstellung der Berichtsvorlage angegebenen Einstellungen ist möglicherweise nur einer dieser Abschnitte vorhanden.

- Abschnitt **Einstellungen**.

  Ändern Sie die Einstellungen des Berichts. Die tatsächliche Auswahl an Einstellungen hängt vom jeweiligen Bericht ab.

- Abschnitt **Sicherheit**. **Einstellungen vom Administrationsserver erben**

  Wenn diese Option aktiviert ist, werden die Sicherheitseinstellungen des Berichts vom Administrationsserver übernommen.

  Wenn diese Option deaktiviert ist, können Sie Sicherheitseinstellungen für den Bericht anpassen. Sie können eine Rolle an einen Benutzer oder eine Gruppe von Benutzern zuweisen oder Berechtigungen für einen Benutzer oder eine Gruppe von Benutzern anwenden (wie für den Bericht).

  Diese Option ist standardmäßig aktiviert.

  Der Abschnitt **Sicherheit** ist verfügbar, wenn im Fenster zur Anpassung der Benutzeroberfläche das Kontrollkästchen **Abschnitte mit Sicherheitseinstellungen anzeigen** aktiviert ist.

- Abschnitt **Hierarchie der Administrationsserver**:

  - **Daten von sekundären und virtuellen Administrationsservern einschließen**

    Wenn diese Option aktiviert ist, umfasst der Bericht die Informationen vom sekundären und vom virtuellen Administrationsserver, die dem Administrationsserver untergeordnet sind, für den die Berichtsvorlage erstellt wurde.

    Deaktivieren Sie diese Option, wenn Sie nur Daten vom aktuellen Administrationsserver anzeigen möchten.

    Diese Option ist standardmäßig aktiviert.

  - **Bis Verschachtelungsebene**

    Der Bericht enthält Daten von sekundären und virtuellen Administrationsservern, die sich unter dem aktuellen Administrationsserver auf der Verschachtelungsebene befinden, die kleiner oder gleich dem angegebenen Wert ist.

    Als Standardwert ist 1 vorgegeben. Sie sollten diesen Wert ändern, wenn Sie Informationen von sekundären Administrationsservern sammeln müssen, die sich auf niedrigeren Ebenen in der Struktur befinden.

  - **Auf Daten warten (Min.)**

    Vor Erstellen des Berichts wartet der Administrationsserver, für den die Berichtsvorlage erstellt wurde, während der angegebenen Anzahl von Minuten auf Daten von sekundären Administrationsservern. Wenn nach Ablauf dieses Zeitraums keine Daten von einem sekundären Administrationsserver eingehen, wird der Bericht dennoch ausgeführt. Anstelle der eigentlichen Daten zeigt der Bericht Daten aus dem Cache (wenn die Option **Cache data from secondary Administration Servers** aktiviert ist) oder **N/A** (nicht verfügbar).

    Der Standardwert beträgt 5 (Minuten).

  - **Daten von sekundären Administrationsservern im Cache zwischenspeichern**

    Sekundäre Administrationsserver übertragen regelmäßig Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Dort werden die übertragenen Daten im Cache gespeichert.

    Wenn der aktuelle Administrationsserver beim Erstellen des Berichts keine Daten von einem sekundären Administrationsserver empfangen kann, zeigt der Bericht Daten aus dem Cache an. Das Datum, an dem die Daten in den Cache übertragen wurden, wird ebenfalls angezeigt.

    Wenn Sie diese Option aktivieren, können Sie die Daten von sekundären Administrationsservern anzeigen, auch wenn die aktuellen Daten nicht mehr abgerufen werden können. Die angezeigten Daten können jedoch veraltet sein.

    Diese Option ist standardmäßig deaktiviert.

  - **Häufigkeit des Cache-Updates (Std.)**

    Sekundäre Administrationsserver übertragen in regelmäßigen Abständen Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Sie können diesen Zeitraum in Stunden angeben. Wenn Sie 0 Stunden angeben, werden die Daten nur übertragen, wenn der Bericht generiert wird.

    Als Standardwert ist 0 vorgegeben.

  - **Detaillierte Informationen von sekundären Administrationsservern übertragen**

    Im generierten Bericht enthält die Tabelle mit den detaillierten Berichtsdaten Daten von sekundären Administrationsservern des Administrationsservers, für den die Berichtsvorlage erstellt wird.

Wenn Sie diese Option aktivieren, wird die Berichtserstellung verlangsamt und der Datenverkehr zwischen den Administrationsservern erhöht. Sie können jedoch alle Daten in einem Bericht anzeigen.

Anstatt diese Option zu aktivieren, möchten Sie möglicherweise detaillierte Berichtsdaten analysieren, um einen fehlerhaften sekundären Administrationsserver zu erkennen und dann denselben Bericht nur für den fehlerhaften Administrationsserver zu generieren.

Diese Option ist standardmäßig deaktiviert.

Erweitertes Filterformat in Berichtsvorlagen

In Kaspersky Security Center 15.1 können Sie ein erweitertes Filterformat auf eine Berichtsvorlage anwenden. Das erweiterte Filterformat bietet im Vergleich mit dem Standardformat eine höhere Flexibilität. Sie können komplexe Filterbedingungen erstellen. Dazu dient eine Auswahl von Filtern, die bei der Berichtserstellung mithilfe des logischen Operators OR auf den Bericht angewandt werden. Hier einige Beispiele:

Filter[1](Feld[1] AND Feld[2]... AND Feld[n]) OR Filter[2](Feld[1] AND Feld[2]... AND Feld[n]) OR... Filter[n](Feld[1] AND Feld[2]... AND Feld[n])

Außerdem können Sie mit dem erweiterten Filterformat ein Zeitintervall festlegen, das ein relatives Zeitformat besitzt (z. B. mithilfe der Bedingung "In den letzten n Tagen") und für spezifische Felder in einem Filter gilt. Die Verfügbarkeit und die Auswahl von Zeitintervall-Bedingungen ist abhängig vom Typ der Berichtsvorlage.

Filter in das erweiterte Filterformat konvertieren

Das erweiterte Filterformat für Berichtsvorlagen wird nur in Kaspersky Security Center 12 und in höheren Versionen unterstützt. Nachdem der Standardfilter in das erweiterte Format konvertiert wurde, ist die Berichtsvorlage nicht mehr mit jenen Administrationsservern in Ihrem Netzwerk kompatibel, auf denen ältere Versionen von Kaspersky Security Center installiert sind. Informationen von diesen Administrationsservern werden nicht in den Bericht aufgenommen.

Um den Standardfilter der Berichtsvorlage in das erweiterte Format zu konvertieren:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie in der Liste der Berichtsvorlagen die gewünschte Berichtsvorlage aus.
4. Wählen Sie im Kontextmenü der gewählten Berichtsvorlage **Eigenschaften** aus.
5. Wählen Sie im daraufhin geöffneten Eigenschaftenfenster auf den Abschnitt **Felder**.
6. Klicken Sie auf der Registerkarte **Detail-Felder** auf den Link **Konvertieren des Filters**.
7. Klicken Sie im folgenden Fenster auf **OK**.

Die Konvertierung einer Berichtsvorlage in das erweiterte Filterformat kann nicht rückgängig gemacht werden. Falls Sie versehentlich auf den Link **Konvertieren des Filters** geklickt haben, können Sie die Änderungen verwerfen. Klicken Sie dazu im Eigenschaftenfenster der Berichtsvorlage auf **Abbrechen**.

8. Um die Änderungen zu übernehmen, schließen Sie das Eigenschaftenfenster der Berichtsvorlage durch Klick auf **OK**.

   Wird das Eigenschaftenfenster der Berichtsvorlage erneut geöffnet, wird der neue Abschnitt **Filter** angezeigt. In diesem Abschnitt können Sie den erweiterten Filter anpassen.

Erweiterten Filter anpassen

Um den erweiterten Filter in den Eigenschaften der Berichtsvorlage anzupassen:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie in der Liste der Berichtsvorlagen jene Berichtsvorlage aus, die zuvor in das erweiterte Filterformat konvertiert wurde.
4. Wählen Sie im Kontextmenü der gewählten Berichtsvorlage **Eigenschaften** aus.
5. Wählen Sie im daraufhin geöffneten Eigenschaftenfenster auf den Abschnitt **Filter**.

   Der Abschnitt **Filter** wird nicht angezeigt, falls die Berichtsvorlage zuvor nicht in das erweiterte Filterformat konvertiert wurde.

   Im Abschnitt **Filter** des Eigenschaftenfensters der Berichtsvorlage können Sie die Liste der auf den Bericht angewandten Filter ändern und einsehen. Jeder Filter in der Liste hat einen einmaligen Namen und entspricht einer Auswahl von Filtern für die entsprechenden Felder in dem Bericht.
6. Öffnen Sie das Fenster mit den Filtereinstellungen auf eine der folgenden Arten:
   - Um einen neuen Filter zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen Filter zu ändern, wählen Sie den gewünschten Filter aus und klicken Sie auf **Ändern**.
7. Wählen Sie im folgenden Fenster die erforderlichen Felder des Filters aus und geben Sie entsprechende Werte an.
8. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster zu schließen.

   Falls Sie einen neuen Filter erstellen, müssen Sie im Feld **Filtername** einen Filternamen angeben, bevor Sie auf **OK** klicken.
9. Schließen Sie das Eigenschaftenfenster der Berichtsvorlage durch Klick auf **OK**.

   Der erweiterte Filter in der Berichtsvorlage ist nun angepasst. Jetzt können Sie mithilfe dieser Berichtsvorlage Berichte erstellen.

Berichte erstellen und anzeigen

Um einen Bericht zu erstellen und anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Doppelklicken Sie in der Liste der Berichtsvorlagen auf die gewünschte Berichtsvorlage.

   Ein Bericht für die ausgewählte Vorlage wird angezeigt.

Im Bericht werden folgende Daten angezeigt:

- Typ und Name des Berichts, eine Kurzbeschreibung und der Berichtszeitraum sowie Informationen darüber, für welche Gerätegruppe der Bericht erstellt wurde.
- Graph-Diagramm mit den repräsentativsten Berichtsdaten.
- Übersichtstabelle mit Kennziffern des Berichts.
- Tabelle mit detaillierten Daten des Berichts.

Bericht speichern

Um den erstellten Bericht zu speichern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie in der Liste der Berichtsvorlagen die gewünschte Berichtsvorlage aus.
4. Wählen Sie im Kontextmenü der gewählten Berichtsvorlage **Speichern** aus.

   Daraufhin wird der Assistent für das Speichern von Berichten gestartet. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird der Ordner geöffnet, in dem die Berichtsdatei gespeichert wurde.

Wenn Sie einen Bericht als xls-Datei speichern, werden alle zugehörigen Bilder, wie das Logo oder Datagramm, als separate Dateien gespeichert.

Aufgabe zum Berichtsversand anlegen

Berichte können per E-Mail versendet werden. Der Versand von Berichten erfolgt in Kaspersky Security Center mithilfe der Aufgabe Berichtsversand.

Um eine Aufgabe für den Versand eines einzelnen Berichts zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie in der Liste der Berichtsvorlagen die gewünschte Berichtsvorlage aus.
4. Wählen Sie im Kontextmenü der gewählten Berichtsvorlage **Berichtsversand** aus.

   Daraufhin wird der Assistent für das Erstellen einer Aufgabe zum Berichtsversand gestartet. Folgen Sie den Anweisungen des Assistenten.

Um eine Aufgabe für den Versand mehrerer Berichte zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur unter dem Knoten mit dem Namen des gewünschten Administrationsservers den Ordner **Aufgaben**.

2. Klicken Sie im Arbeitsbereich des Ordners **Aufgaben** auf die Schaltfläche **Aufgabe erstellen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Die erstellte Aufgabe Berichtsversand wird im Ordner **Aufgaben** der Konsolenstruktur angezeigt.

Die Aufgabe zum Berichtsversand wird automatisch angelegt, wenn bei der Installation von Kaspersky Security Center die E-Mail-Einstellungen festgelegt wurden.

Schritt 1. Auswählen des Aufgabentyps

Wählen Sie im Fenster **Aufgabentyp auswählen**, in der Liste der Aufgaben, den Aufgabentyp **Berichtsversand**.

Klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.

Schritt 2. Auswählen des Berichtstyps

Wählen Sie im Fenster **Berichtstyp auswählen** in der Liste der Vorlagen für das Erstellen einer Aufgabe den Berichtstyp aus.

Klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.

Schritt 3. Vorgänge mit Berichten

Geben Sie in dem Fenster **Aktion für Berichte auswählen** die folgenden Einstellungen an:

- **Berichte per E-Mail versenden**

  Wenn diese Option aktiviert ist, versendet das Programm die erstellten Berichte per E-Mail.

  Die Einstellungen für das Senden eines Berichts per E-Mail können Sie durch Klicken auf den Link **Einstellungen für den Versand per E-Mail** anpassen. Der Link ist verfügbar, wenn die Option aktiviert ist.

  Ist die Option deaktiviert, speichert das Programm Berichte im für die Speicherung von Berichten angegebenen Ordner.

  Diese Option ist standardmäßig deaktiviert.

- **Berichte im freigegebenen Ordner speichern**

  Wenn die Option aktiviert ist, speichert das Programm Berichte in dem im Feld unter dem Kontrollkästchen angegebenen Ordner. Um Berichte in einem freigegebenen Ordner zu speichern, geben Sie den UNC-Pfad zu diesem Ordner an. In diesem Fall müssen für den Zugriff auf diesen Ordner im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** das Benutzerkonto und das Kennwort des Benutzers angegeben werden.

  Ist die Option deaktiviert, werden Berichte nicht im Ordner gespeichert, sondern per E-Mail versendet.

  Diese Option ist standardmäßig deaktiviert.

- **Existierende Berichte vom gleichen Typ ersetzen**

  Wenn diese Option aktiviert ist, wird die im Ordner für die Speicherung von Berichtsdateien beim vorherigen Aufgabenstart gespeicherte Datei bei jedem Aufgabenstart durch eine neue Berichtsdatei ersetzt.

  Ist die Option deaktiviert, werden die Berichtsdateien nicht überschrieben. Bei jedem Aufgabenstart wird im Ordner eine einzelne Berichtsdatei gespeichert.

Das Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Bericht im folgenden Ordner speichern** aktiviert ist.

Diese Option ist standardmäßig deaktiviert.

- **Benutzerkonto für den Zugriff auf den gemeinsamen Ordner angeben**

  Wenn die Option aktiviert ist, können Sie das Konto angeben, unter dem der Bericht gespeichert werden soll. Wenn im Fenster **Aktionen mit Berichten** als Einstellung **Bericht im folgenden Ordner speichern** der UNC-Pfad des freigegebenen Ordners angegeben ist, müssen das Benutzerkonto und das Kennwort für den Zugriff auf diesen Ordner angegeben werden.

  Ist die Option deaktiviert, wird der Bericht unter dem Konto des Administrationsservers in den Ordner geschrieben.

  Das Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Bericht im folgenden Ordner speichern** aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

Wenn Sie einen Bericht als xls-Datei speichern oder versenden, werden alle zugehörigen Bilder, wie das Logo oder Datagramm, als separate Dateien gespeichert.

Klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.

Schritt 4. Auswählen des Kontos für Aufgabenausführung

Im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** können Sie festlegen, unter welchem Benutzerkonto die Aufgabe gestartet wird. Wählen Sie eine der folgenden Varianten aus:

- **Standardbenutzerkonto**

  Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

  Diese Variante ist standardmäßig ausgewählt.

- **Benutzerkonto festlegen**

  Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

  - **Benutzerkonto**

    Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

  - **Kennwort**

    Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

Klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.

Schritt 5. Konfigurieren eines Aufgabenzeitplans

Auf der Seite **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

- **Start nach Zeitplan**

  Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

  - **Alle n Stunden**

    Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

    Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

  - **Alle n Tage**

    Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

    Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

  - **Alle n Wochen**

    Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

    Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

  - **Alle n Minuten**

    Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

    Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

  - **Täglich (Sommerzeit wird nicht unterstützt)**

    Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

    Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

    Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

  - **Wöchentlich**

    Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

  - **Nach Wochentagen**

    Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

    Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

  - **Monatlich**

    Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

- Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
- Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

  Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
- Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

Schritt 6. Festlegen des Aufgabennamens

Geben Sie im Fenster **Aufgabenname festlegen** den Namen der Regel an, die Sie erstellen. Der Aufgabenname darf höchstens 100 Zeichen lang sein und keine Sonderzeichen (wie `"*<>?\:|`) enthalten.

Klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.

Schritt 7. Abschließen der Aufgabenerstellung

Klicken Sie im Fenster **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistent abzuschließen.

Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Arbeiten mit statistischen Daten

Statistische Informationen über den Status des Schutzsystems und der verwalteten Geräte werden als anpassbare Informationsbereiche dargestellt. Die Statistik wird im Arbeitsbereich des Knotens **Administrationsserver** auf der Registerkarte **Statistik** angezeigt. Die Registerkarte enthält mehrere untergeordnete Registerkarten (Seiten). Auf jeder Registerkartenseite wird ein Informationsbereich mit statistischen Informationen sowie Links auf Neuigkeiten und andere Materialien von Kaspersky angezeigt. Statistikdaten werden in den Informationsbereichen als Kreis- oder Säulendiagramme oder Tabellen dargestellt. Daten in den Informationsbereichen werden während der Ausführung des Programms aktualisiert und spiegeln den aktuellen Status der Sicherheitsanwendung wieder.

Sie können die Zusammenstellung der auf der Registerkarte **Statistik** enthaltenen untergeordneten Registerkarten, die Auswahl der Informationsbereiche auf jeder Registerkartenseite sowie die Darstellungsweise der Daten in den Informationsbereichen ändern.

*Um auf der Registerkarte **Statistik** eine neue untergeordnete Registerkarte mit Informationsbereichen hinzuzufügen, gehen Sie folgendermaßen vor:*

1. Klicken Sie auf die Schaltfläche **Ansicht konfigurieren** in der rechten oberen Ecke der Registerkarte **Statistik**.

   Das Fenster der Statistikeigenschaften wird geöffnet. Dieses Fenster enthält eine Liste von Registerkartenseiten, die derzeit auf der Registerkarte **Statistik** angezeigt werden. Sie können im Fenster die Anzeigereihenfolge der Fenster auf der Registerkarte ändern, Seiten hinzufügen und entfernen und mithilfe der Schaltfläche **Eigenschaften** zu den Seiteneigenschaften wechseln.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird das Eigenschaftenfenster der neuen Seite geöffnet.

3. Konfigurieren Sie die neue Seite:

   - Geben Sie im Abschnitt **Allgemein** den Namen der Seite an.

   - Fügen Sie im Abschnitt **Informationsbereiche** mithilfe der Schaltfläche **Hinzufügen** Informationsbereiche hinzu, die auf der Seite angezeigt werden sollen.

     Mithilfe der Schaltfläche **Eigenschaften** im **Informationsbereiche** können Sie die Eigenschaften der hinzugefügten Informationsbereiche anpassen: Name, Typ und Art des Diagramms im Bereich, Daten für die Erstellung des Diagramms.

4. Klicken Sie auf die Schaltfläche **OK**.

Die hinzugefügte Registerkartenseite mit Informationsbereichen wird auf der Registerkarte **Statistik** angezeigt. Mithilfe des Symbols Einstellungen (⚙) können Sie rasch zwischen der Seitenkonfiguration und dem ausgewählten Informationsbereich auf der Seite wechseln.

Benachrichtigungseinstellungen für Ereignisse anpassen

Kaspersky Security Center ermöglicht die Auswahl der Benachrichtigungsmethode für Ereignisse für den Administrator auf den Client-Geräten und die Anpassung der Benachrichtigungseinstellungen:

- E-Mail. Beim Auftreten eines Ereignisses sendet das Programm Benachrichtigungen an die angegebenen E-Mail-Adressen. Der Text der Benachrichtigung kann angepasst werden.
- SMS. Beim Auftreten eines Ereignisses sendet das Programm Benachrichtigungen an die angegebenen Telefonnummern. Sie können die SMS-Benachrichtigungen konfigurieren, die über das Mail Gateway gesendet werden.
- Ausführbare Datei Beim Auftreten eines Ereignisses auf dem Gerät wird auf dem Administrator-Arbeitsplatz eine ausführbare Datei gestartet. Mithilfe der ausführbaren Datei erhält der Administrator die Parameter des eingetretenen Ereignisses.

Um die Einstellungen für Benachrichtigungen über Ereignisse auf den Client-Geräten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Klicken Sie auf den Link **Benachrichtigungseinstellungen und Ereignis-Export anpassen** und wählen Sie in der Dropdown-Liste die Option **Benachrichtigungseinstellungen anpassen**.

   Daraufhin wird das Fenster **Eigenschaften: Ereignisse** geöffnet.
4. Wählen Sie im Abschnitt **Benachrichtigung** eine Benachrichtigungsmethode aus (E-Mail, SMS, Start einer ausführbaren Datei) und passen Sie die Benachrichtigungseinstellungen an:

   - **E-Mail**

     Auf der Registerkarte **E-Mail** können Sie die E-Mail-Benachrichtigung für Ereignisse konfigurieren.

     Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen.

     Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

     - IPv4- oder IPv6-Adresse
     - Windows-Netzwerkname (NetBIOS-Name) des Geräts
     - DNS-Name des SMTP-Servers

     Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig wird Portnummer 25 verwendet.

Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren, können Sie mehrere MX-Einträge von IP-Adressen für denselben DNS-Namen des SMTP-Servers verwenden. Der gleiche DNS-Name kann mehrere MX-Einträge mit unterschiedlichen Prioritäten für das Empfangen von E-Mail-Nachrichten enthalten. Der Administrationsserver versucht, entsprechend der Priorität der MX-Einträge, die E-Mail-Nachrichten in aufsteigender Reihenfolge an den SMTP-Server zu senden. Diese Option ist standardmäßig deaktiviert.

Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren und die Verwendung von TLS-Einstellungen deaktivieren, ist es empfehlenswert, die DNSSEC-Einstellungen auf Ihrem Servergerät als zusätzliche Schutzmaßnahme beim Senden von E-Mail-Nachrichten zu verwenden.

Klicken Sie auf den Link **Einstellungen**, um zusätzliche Benachrichtigungseinstellungen zu definieren:

- Betreff (Betreff einer E-Mail-Nachricht)
- E-Mail-Adresse des Absenders
- ESMTP-Authentifizierungseinstellungen

Sie müssen ein Konto für die Authentifizierung auf einem SMTP-Server angeben, wenn die Option zur ESMTP-Authentifizierung für dem SMTP-Server aktiviert ist.

- TLS-Einstellungen für den SMTP-Server:
  - **Kein TLS verwenden**

    Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.
  - **TLS verwenden, wenn vom SMTP-Server unterstützt**

    Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.
  - **TLS immer verwenden und Serverzertifikat auf Gültigkeit prüfen**

    Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **TLS immer verwenden und Serverzertifikat auf Gültigkeit prüfen** auswählen, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können die TLS-Einstellungen für einen SMTP-Server angeben:

- Geben Sie eine Datei mit SMTP-Server-Zertifikat an:

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center prüft, ob das Zertifikat eines SMTP-Servers auch von eine vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

- Geben Sie die Datei des Client-Zertifikats an:

Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen Zertifizierungsstelle. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

- X-509-Zertifikat:

Sie müssen eine Datei mit dem Zertifikat und eine Datei mit dem privaten Schlüssel angeben. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Laden der Dateien ist spielt keine Rolle. Wenn beide Dateien geladen sind, müssen Sie das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- pkcs12-Container:

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

Das Feld **Benachrichtigungstext** enthält Standard-Text mit der Information zum Ereignis, der beim Eintreten des Ereignisses versendet wird. Dieser Text enthält Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne. Sie können den Text der Meldung bearbeiten und weitere Platzhalter mit relevanten Informationen über das Ereignis hinzufügen. Klicken Sie auf die Schaltfläche rechts neben dem Feld, um eine Liste mit verfügbaren Platzhaltern anzuzeigen.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Klicken Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren**, um die maximale Anzahl an Benachrichtigungen anzugeben, die das Programm während des angegebenen Zeitintervalls versenden darf.

Klicken Sie auf die Schaltfläche **Testnachricht senden**, um zu überprüfen, ob Sie die Benachrichtigungen richtig konfiguriert haben. Das Programm sollte eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen senden.

- **SMS**

Auf der Registerkarte **SMS** können Sie den Versand von SMS-Benachrichtigungen zu verschiedenen Ereignissen an ein Mobiltelefon anpassen. SMS-Nachrichten werden über ein Mail-Gateway gesendet.

Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen ein, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen. Die Benachrichtigungen werden an die Telefonnummern gesendet, die den angegebenen E-Mail-Adressen zugewiesen sind.

Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- Windows-Netzwerkname (NetBIOS-Name) des Geräts
- DNS-Name des SMTP-Servers

Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Ports für die Kommunikation eines SMTP-Servers an. Standardmäßig wird Portnummer 25 verwendet.

Klicken Sie auf den Link **Einstellungen**, um zusätzliche Benachrichtigungseinstellungen zu definieren:

- Betreff (Betreff einer E-Mail-Nachricht)
- E-Mail-Adresse des Absenders
- ESMTP-Authentifizierungseinstellungen

Falls erforderlich, können Sie ein Konto für die Authentifizierung auf einem SMTP-Server angeben, wenn die Option zur ESMTP-Authentifizierung für einen SMTP-Server aktiviert ist.

- TLS-Einstellungen für einen SMTP-Server

Sie können entweder die Verwendung von TLS deaktivieren, TLS verwenden, wenn der SMTP-Server dieses Protokoll unterstützt, oder die Verwendung von TLS erzwingen. Wenn Sie nur TLS verwenden möchten, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie in dem Fall, dass Sie nur TLS verwenden möchten, ein Zertifikat für die Client-Authentifizierung am SMTP-Server angeben.

- Geben Sie eine Datei mit SMTP-Server-Zertifikat an

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von einer vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei in Kaspersky Security Center hochladen. Kaspersky Security Center prüft, ob das Zertifikat des SMTP-Servers auch von einer vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu dem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von einer vertrauenswürdigen Zertifizierungsstelle kommt.

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist. Das Feld **Benachrichtigungstext** enthält Standard-Text mit der Information zum Ereignis, der beim Eintreten des Ereignisses versendet wird. Dieser Text enthält Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne. Sie können den Text der Meldung bearbeiten und weitere Platzhalter mit relevanten Informationen über das Ereignis hinzufügen. Klicken Sie auf die Schaltfläche rechts neben dem Feld, um eine Liste mit verfügbaren Platzhaltern anzuzeigen.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Klicken Sie auf den Link **Beschränkung für Anzahl der Benachrichtigungen konfigurieren**, um die maximale Anzahl an Benachrichtigungen anzugeben, die das Programm während des angegebenen Zeitintervalls versenden darf.

Klicken Sie auf die Schaltfläche **Testnachricht senden** um zu überprüfen, ob Sie die Benachrichtigungen richtig konfiguriert haben. Das Programm sollte eine Testnachricht an den von Ihnen angegebenen Empfänger senden.

- **Start einer ausführbaren Datei**

  Wenn diese Methode der Zustellung von Benachrichtigungen ausgewählt ist, können Sie im Eingabefeld das Programm angeben, das gestartet wird, sobald ein Ereignis eintritt.

  Wenn Sie auf den Link **Beschränkung für Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, die das Programm innerhalb des angegebenen Zeitintervalls versenden darf.

  Klicken Sie auf die Schaltfläche **Testnachricht senden**, um zu prüfen, ob Sie die Benachrichtigungen korrekt konfiguriert haben: Das Programm sendet dann eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen.

5. Geben Sie im Feld **Benachrichtigungstext** den Text ein, den das Programm bei Eintreten eines Ereignisses versenden wird.

   Aus der Dropdown-Liste rechts vom Textfeld können in die Nachricht Platzhalter für zusätzliche Einstellungen mit den Ereignisdetails (wie Beschreibung, Eintrittszeit des Ereignisses und sonstiges) hinzugefügt werden.

   > Wenn der Benachrichtigungstext das Zeichen % enthält, muss es zweimal angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

6. Überprüfen Sie über die Schaltfläche **Testnachricht senden**, ob die Benachrichtigungen richtig eingestellt wurden.

   Das Programm sendet eine Testbenachrichtigung an den angegebenen Empfänger.

7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Daraufhin werden die angepassten Einstellungen der Benachrichtigung auf alle Ereignisse übernommen, die auf den Client-Geräten auftreten.

Sie können die Benachrichtigungseinstellungen für bestimmte Ereignisse im Abschnitt **Konfiguration von Ereignissen** in den Einstellungen des Administrationsservers für eine Richtlinieneinstellung oder eine Programmeinstellung überschreiben.

Zertifikat für SMTP-Server erstellen

Um ein Zertifikat für einen SMTP-Server zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Klicken Sie auf den Link **Benachrichtigungseinstellungen und Ereignis-Export anpassen** und wählen Sie in der Dropdown-Liste die Option **Benachrichtigungseinstellungen anpassen**.

   Das Eigenschaftenfenster des Ereignisses wird geöffnet.

4. Wählen Sie auf der Registerkarte **E-Mail** mithilfe des Links **Einstellungen** das Fenster **Einstellungen**.
5. Öffnen Sie im Fenster **Einstellungen** mithilfe des Links **Angabe des Zertifikats** das Fenster **Zertifikat für die Signatur**.
6. Klicken Sie im Fenster **Zertifikat für die Signatur** auf **Durchsuchen**.

   Das Fenster **Zertifikat** wird geöffnet.

7. Wählen Sie im Dropdown-Feld **Zertifikatstyp** entweder einen offenen oder geschlossenen Zertifikatstyp aus:

   - Wenn ein geschlossener Zertifikatstyp ausgewählt ist (**Container PKCS#12**), geben Sie die Zertifikatsdatei und das Kennwort an.

   - Wenn ein offener Zertifikatstyp ausgewählt ist (**X.509-Zertifikat**):

     a. Geben Sie die Datei des privaten Schlüssels an (Datei mit der Erweiterung *prk oder *.pem).

     b. Geben Sie das Kennwort des privaten Schlüssels an.

     c. Geben Sie die Datei des öffentlichen Schlüssels an (Datei mit der Erweiterung cer).

8. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin wird ein Zertifikat für den SMTP-Server ausgestellt.

Ereignisauswahlen

Informationen über Ereignisse bei der Ausführung von Kaspersky Security Center und der verwalteten Programme werden sowohl in der Administrationsserver-Datenbank als auch im Microsoft Windows-Systemprotokoll gespeichert. Sie können die Informationen aus der Administrationsserver-Datenbank im Arbeitsbereich des Knotens **Administrationsserver** auf der Registerkarte **Ereignisse** anzeigen lassen.

Die Informationen auf der Registerkarte **Ereignisse** werden in Form einer Liste mit Ereignisauswahlen angezeigt. Jede Auswahl umfasst nur Ereignisse eines bestimmten Typs. Beispielsweise enthält die Auswahl "Gerätestatus – Kritisch" nur Einträge über Änderungen des Gerätestatus auf "Kritisch". Nach der Installation des Programms sind auf der Registerkarte **Ereignisse** eine Reihe von Standardereignisauswahlen enthalten. Sie können zusätzliche (benutzerdefinierte) Ereignisauswahlen erstellen sowie Informationen über Ereignisse in eine Datei exportieren.

Ereignisauswahl anzeigen

Um sich eine Ereignisauswahl anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.

3. Wählen Sie in der Dropdown-Liste **Ereignisauswahlen** die gewünschte Ereignisauswahl aus.

   Wenn Sie möchten, dass die Ereignisse dieser Auswahl dauerhaft im Arbeitsbereich angezeigt werden, klicken Sie auf das Stern-Symbol (☆) neben der Auswahl.

   Daraufhin wird im Arbeitsbereich die Liste der Ereignisse des gewählten Typs angezeigt, die auf dem Administrationsserver gespeichert werden.

Sie können die Informationen in der Ereignisliste in einer beliebigen Spalte der Liste in auf- oder absteigender Reihenfolge sortieren.

Einstellungen für Ereignisauswahl anpassen

Um die Einstellungen für eine Ereignisauswahl anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Öffnen Sie die gewünschte Ereignisauswahl auf der Registerkarte **Ereignisse**.
4. Klicken Sie auf die Schaltfläche **Auswahleigenschaften**.

Im folgenden Eigenschaftenfenster der Ereignisauswahl können Sie die Einstellungen der Auswahl anpassen.

Ereignisauswahl erstellen

Um eine Ereignisauswahl zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Klicken Sie auf die Schaltfläche **Auswahl erstellen**.
4. Geben Sie im folgenden Fenster **Neue Ereignisauswahl** den Namen der zu erstellenden Auswahl an, und klicken Sie auf **OK**.

Daraufhin wird in der Dropdown-Liste **Ereignisauswahlen** eine Auswahl mit dem von Ihnen angegebenen Namen erstellt.

Die erstellte Ereignisauswahl enthält standardmäßig alle Ereignisse, die auf dem Administrationsserver gespeichert werden. Damit bestimmte Ereignisse in der Auswahl angezeigt werden, konfigurieren Sie die Einstellungen der Auswahl.

Ereignisauswahl in eine Textdatei exportieren

Um eine Ereignisauswahl in eine Datei zu exportieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Klicken Sie auf die Schaltfläche **Import/Export**.
4. Wählen Sie in der Dropdown-Liste die Option **Ereignisse in Datei exportieren**.

Daraufhin wird der Assistent für den Ereignis-Export gestartet. Folgen Sie den Anweisungen des Assistenten.

Ereignisse aus einer Auswahl löschen

Um Ereignisse aus der Auswahl zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des relevanten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Wählen Sie mit der Maus und den Tasten **Umschalt** oder **Strg** die Ereignisse aus, die gelöscht werden sollen.
4. Löschen Sie die gewählten Ereignisse auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf ein beliebiges Ereignis und wählen Sie **Löschen**.

     Mit der Auswahl **Alle löschen** werden aus der Auswahl alle angezeigten Ereignisse gelöscht, und zwar unabhängig davon, welche Ereignisse zuvor zum Löschen gewählt wurden.

   - Klicken Sie im Informationsfeld mit den gewählten Ereignissen auf den Link **Ereignis löschen** (wenn ein einziges Ereignis gewählt wurde) oder auf den Link **Ereignisse löschen** (wenn mehrere Ereignisse gewählt wurden).

Daraufhin werden die ausgewählten Ereignisse gelöscht.

Programme auf Anfrage von Benutzern zu Ausschlüssen hinzufügen

Wenn Sie Benutzeranfragen erhalten, welche die Freigabe irrtümlich blockierter Programme beantragen, können Sie für diese Programme einen Ausschluss aus den Regeln zur Adaptiven Sicherheit erstellen. Daraufhin werden diese Programme auf den Geräten der Benutzer nicht länger blockiert. Sie können die Anzahl der Benutzeranfragen auf der Registerkarte **Überwachung** des Administrationsservers verfolgen.

Um Programme, die von Kaspersky Endpoint Security verboten wurden, auf Benutzeranfrage hin zu Ausschlüssen hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Ereignisse** aus.
3. Wählen Sie in der Dropdown-Liste **Ereignisauswahlen** die Option **Benutzeranfragen**.
4. Klicken Sie mit der rechten Maustaste auf die Benutzeranfrage bzw. die Benutzeranfragen mit Programmen, die Sie zu Ausschlüssen hinzufügen möchten, und wählen Sie dann **Ausschluss hinzufügen**.

   Daraufhin wird der Assistent für das Hinzufügen eines Ausschlusses gestartet. Folgen Sie seinen Anweisungen.

Nach der nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver werden die ausgewählten Apps aus der Liste **Auslöser der Regel im Smart-Training-Status** (unter **Datenverwaltung** in der Konsolenstruktur) ausgeschlossen und nicht mehr in der Liste angezeigt.

Geräteauswahlen

Informationen zum Status der Geräte und mobiler Geräte finden Sie in der Konsolenstruktur im Ordner **Geräteauswahlen**.

Die Informationen im Ordner **Geräteauswahlen** sind in Form einer Liste der Geräteauswahlen dargestellt. Jede Auswahl beinhaltet Geräte, die bestimmten Bedingungen entsprechen. Beispielsweise enthält die Auswahl **Geräte mit dem Status "Kritisch"** nur die Geräte mit dem Status *Kritisch*. Nach Installation des Programms wird in dem Ordner **Geräteauswahlen** eine Reihe von Standardauswahlen angezeigt. Sie können zusätzliche (benutzerdefinierte) Geräteauswahlen erstellen, Einstellungen für Auswahlen in eine Datei exportieren und Auswahlen mit den aus einer Datei importierten Einstellungen erstellen.

Geräteauswahl anzeigen

Um eine Geräteauswahl anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Wählen Sie die gewünschte Geräteauswahl im Arbeitsbereich des Ordners aus der Liste **Geräte der Auswahl** aus.
3. Klicken Sie auf die Schaltfläche **Auswahl starten**.
4. Klicken Sie auf die Registerkarte **Ergebnisse der Auswahl**.

Daraufhin wird im Arbeitsbereich die Liste der Geräte angezeigt, die den Einstellungen der Auswahl entsprechen.

Sie können die Informationen in der Geräteliste in einer beliebigen Spalte in auf- oder absteigender Reihenfolge sortieren.

Einstellungen einer Geräteauswahl anpassen

Um die Einstellungen für eine Geräteauswahl anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Klicken Sie im Arbeitsbereich auf die Registerkarte **Auswahl** und klicken Sie dann auf die passende Geräteauswahl in der Liste der benutzerdefinierten Auswahlen.
3. Klicken Sie auf die Schaltfläche **Auswahleigenschaften**.

4. Passen Sie im nächsten Eigenschaftenfenster folgende Einstellungen an:

   - Allgemeine Auswahleigenschaften.
   - Bedingungen, die erfüllt sein müssen, damit Geräte in die Auswahl aufgenommen werden. Sie können die Bedingungen anpassen, sobald Sie den Namen der Bedingung festlegen und auf **Eigenschaften** klicken.
   - Sicherheitseinstellungen.

5. Klicken Sie auf die Schaltfläche **OK**.

Die Einstellungen werden übernommen und gespeichert.

Nachfolgende werden die Einstellungen für Bedingungen der Aufnahme von Geräten in die Auswahl beschrieben. Die Bedingungen beruhen auf dem logischen ODER: In die Auswahl werden nur Geräte aufgenommen, die mindestens eine Bedingung erfüllen.

Allgemein

Im Abschnitt **Allgemein** kann der Name der Auswahlbedingung geändert sowie bestimmt werden, ob diese Auswahlbedingung umgekehrt werden soll:

Auswahlbedingung umkehren

Diese Option ist standardmäßig deaktiviert.

Wenn Sie diese Option aktivieren, wird die vorgegebene Auswahlbedingung umgekehrt. Alle Geräte, die diese Bedingung nicht erfüllen, werden in die Auswahl aufgenommen.

Das folgende Beispiel erläutert die Logik einer Inversion:

- **Bedingung**: Auf Ihrem Gerät befindet sich ein Betriebssystem, das zu den Linux-Systemen gehört und die Build-Nummer 00.0.000 besitzt.
- **Invertierter Zustand**: Auf Ihrem Gerät befindet sich ein Betriebssystem, dass NICHT (zu den Linux-Systemen gehört und die Build-Nummer 00.0.000 besitzt), was Folgendem entspricht:

  Es ist ein Betriebssystem vorhanden, das NICHT zu den Linux-Systemen gehört ODER das NICHT die Build-Nummer 00.0.000 besitzt.

Die Auswahl umfasst also beispielhaft Geräte mit Windows-Betriebssystemen mit der Build-Nummer 00.0.000 oder Geräte mit Linux-Betriebssystemen mit einer Build-Nummer, die von 00.0.000 abweicht.

Netzwerk

Im Abschnitt **Netzwerk** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkdaten konfigurieren:

- **Gerätename oder IP-Adresse**

  Windows-Netzwerkname (NetBIOS-Name) des Geräts oder die IPv4- oder IPv6-Adresse.

- **Windows-Domäne**

  Es werden Geräte angezeigt, die zur angegebenen Windows-Domäne gehören.

- **Administrationsgruppe**

  Es werden Geräte angezeigt, die zur angegebenen Administrationsgruppe gehören.

- **Beschreibung**

  Text, der im Eigenschaftenfenster des Geräts enthalten ist: im Feld **Beschreibung** des Abschnitts **Allgemein**.

  Für die Beschreibung eines Textes im Feld **Beschreibung** sind die folgenden Zeichen zulässig:

  - Innerhalb eines Wortes:

    - *****. Dieses Zeichen ersetzt beliebige Ausdrücke mit einer beliebigen Zahl von Zeichen.

    Beispiel:

    Für die Beschreibung der Wörter **Server** und **Server-**können Sie die Zeichenfolge **Server*** verwenden.

    - **?.** Dieses Zeichen ersetzt ein beliebiges Symbol.

    Beispiel:

    Für die Beschreibung der Wörter **Regel** oder **Regeln** können Sie die Zeichenfolge **Regel?** verwenden.

    Das Zeichen ***** oder **?** kann nicht als das erste Zeichen in einer Textbeschreibung verwendet werden.

  - Zur Verknüpfung mehrerer Wörter:

    - Leerzeichen: Es werden alle Geräte angezeigt, deren Beschreibung ein beliebiges der angegebenen Wörter enthält.

    Beispiel:

    Zur Beschreibung einer Phrase, die entweder das Wort **Sekundär** oder **Virtuell** enthält, können Sie die Zeichenfolge **Sekundär Virtuell** verwenden.

    - **+**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss.

    Beispiel:

    Zur Beschreibung einer Phrase, welche die beiden Wörter **Sekundär** und **Virtuell** enthält, können Sie den Ausdruck **+Sekundär+Virtuell** verwenden.

    - **-**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf.

    Beispiel:

    Zur Beschreibung einer Phrase, die das Wort **Sekundär** enthält, jedoch das Wort **Virtuell** nicht enthalten darf, können Sie den Ausdruck **+Sekundär-Virtuell** verwenden.

    - **"<Textabschnitt>"**: Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein.

    Beispiel:

    Zur Beschreibung einer Phrase, welche die Wortverbindung **Sekundärer Server** enthält, können Sie den Ausdruck **"Sekundärer Server"** verwenden.

- **IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

  Diese Option ist standardmäßig deaktiviert.

Tags

Im Abschnitt **Tags** können Sie Bedingungen für die Aufnahme von Geräten in die Auswahl nach Schlüsselworten (Tags) anpassen, die zuvor zu den Beschreibungen der verwalteten Geräte hinzugefügt wurden:

- **Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft**

  Ist die Option aktiviert, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibungen zumindest einer der gewählten Tags vorhanden ist.

  Ist die Option deaktiviert, werden in den Suchergebnissen nur Geräte angezeigt, in deren Beschreibungen alle gewählten Tags vorhanden sind.

  Diese Option ist standardmäßig deaktiviert.

- **Der Tag muss vorhanden sein**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

  Diese Variante ist standardmäßig ausgewählt.

- **Der Tag darf nicht vorhanden sein**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag nicht vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

Active Directory

Im Abschnitt **Active Directory** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand ihrer Active Directory-Daten konfigurieren:

- **Das Gerät befindet sich in einer Active Directory-Organisationseinheit**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Active Directory-Organisationseinheit aufgenommen, das im Eingabefeld angegeben wurde.

  Diese Option ist standardmäßig deaktiviert.

- **Untergeordnete Organisationseinheiten einschließen**

  Wenn die Option aktiviert ist, werden die Geräte aus allen untergeordneten Organisationseinheiten der angegebenen Domänen-Organisationseinheit aufgenommen.

  Diese Option ist standardmäßig deaktiviert.

- **Dieses Gerät gehört zu einer Active-Directory-Gruppe**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Active-Directory-Gruppe aufgenommen, die im Eingabefeld angegeben wurde.

Diese Option ist standardmäßig deaktiviert.

Netzwerkaktivität

Im Abschnitt **Netzwerkaktivität** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkaktivitäten konfigurieren:

- **Dieses Gerät ist ein Verteilungspunkt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die als Verteilungspunkte fungieren, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die als Verteilungspunkte fungieren, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Verbindung mit Administrationsserver nicht trennen**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Aktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** aktiviert ist.
  - **Deaktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** deaktiviert ist.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Das Verbindungsprofil wurde gewechselt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Letzte Verbindung mit dem Administrationsserver**

  Mithilfe dieses Kontrollkästchens können Sie ein Kriterium für die Suche von Geräten anhand des Zeitpunkts der letzten Verbindung mit dem Administrationsserver ausführen.

  Wenn dieses Kontrollkästchen aktiviert ist, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, während dessen die letzte Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver hergestellt wurde. Bei Auswahl dieser Option werden in die Auswahl Geräte aufgenommen, die dem festgelegten Zeitraum entsprechen.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Neue Geräte bei der Netzwerkabfrage erkannt**

  Suche nach neuen Geräten, die während der letzten Tage bei der Netzwerkabfrage gefunden wurden.

  Wenn diese Option aktiviert ist, umfasst die Auswahl nur neue Geräte, die bei einer Gerätesuche während der im Feld **Erkennungszeitraum (Tage)** angegebenen Anzahl von Tagen gefunden wurden.

  Ist die Option deaktiviert, umfasst die Auswahl alle Geräte, die bei einer Gerätesuche gefunden wurden.

  Diese Option ist standardmäßig deaktiviert.

- **Gerät ist sichtbar**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Es werden Geräte in die Auswahl aufgenommen, die momentan im Netzwerk sichtbar sind.
  - **Nein**. Die Anwendung nimmt Geräte in die Auswahl auf, die momentan nicht im Netzwerk sichtbar sind.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Programm

Im Abschnitt **Programm** können Sie die Kriterien für die Aufnahme von Geräten anhand des ausgewählten verwalteten Programms konfigurieren:

- **Programmname**

  In der Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl wählen, wenn die Suche anhand des Namens der Kaspersky-Anwendung erfolgt.

  In der Liste sind nur die Anwendungen aufgeführt, für die Verwaltungs-Plug-ins im Administrator-Arbeitsplatz installiert sind.

  Wurde keine Anwendung gewählt, wird kein Kriterium angewandt.

- **Programmversion**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach Versionsnummer der Kaspersky-Anwendung erfolgt.

  Wurde keine Versionsnummer angegeben, wird kein Kriterium angewandt.

- **Name des kritischen Updates**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach dem Namen der Anwendung oder nach der Update-Paketnummer erfolgt.

  Ist dieses Feld leer, wird kein Kriterium angewandt.

- **Letztes Update der Module**

  Mithilfe dieser Option können Sie ein Kriterium für die Suche nach Geräten nach Uhrzeit des letzten Updates der Anwendungsmodule angeben, die auf den Geräten installiert wurden.

  Ist das Kontrollkästchen aktiviert, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, in dem das letzte Update der auf den Geräten installierten Anwendungsmodule ausgeführt wurde.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Gerät wird über Kaspersky Security Center verwaltet**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, die über Kaspersky Security Center verwaltet werden:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn sie über Kaspersky Security Center verwaltet werden.
  - **Nein**. Das Programm nimmt Geräte in die Auswahl auf, wenn sie nicht über Kaspersky Security Center verwaltet werden.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Sicherheitsanwendung ist installiert**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, auf denen eine Sicherheitsanwendung installiert wurde:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn auf ihnen eine Sicherheitsanwendung installiert ist.
  - **Nein**. Die Anwendung nimmt alle Geräte in die Auswahl auf, die keine Sicherheitsanwendung installiert haben.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Betriebssystem

Im Abschnitt **Betriebssystem** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl auf der Grundlage des darauf installierten Betriebssystems anpassen.

- **Version des Betriebssystems**

  Ist das Kontrollkästchen aktiviert, können Sie Betriebssysteme in der Liste auswählen. Geräte, auf denen die angegebenen Betriebssysteme installiert sind, werden in die Suchergebnisse aufgenommen.

- **Bitzahl des Betriebssystems**

  In dieser Dropdown-Liste können Sie die Architektur des Betriebssystems auswählen, die vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird (**Unbekannt**, **x86**, **AMD64**, **IA64**). Standardmäßig ist in dieser Liste keine Variante ausgewählt, die Architektur des Betriebssystems ist nicht angegeben.

- **Service Pack-Version des Betriebssystems**

  In diesem Feld können Sie die Service Pack-Version (im Format *X.Y*) des Betriebssystems angeben, die bestimmt, wie die Verschiebungsregel auf das Gerät angewendet wird. Standardmäßig ist keine Version angegeben.

- **Build-Version des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Versionsnummer des Betriebssystems. Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Suche nach allen Versionsnummern mit Ausnahme der angegebenen anpassen.

- **Release-ID des Betriebssystems**

  Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Release-Identifikator (ID) des Betriebssystems Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-ID haben muss. Sie können auch eine Suche nach allen Release-ID-Nummern mit Ausnahme der angegebenen anpassen.

Gerätestatus

Im Abschnitt **Gerätestatus** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Beschreibung des Gerätestatus des verwalteten Programms anpassen:

- **Gerätestatus**

  In dieser Dropdown-Liste können Sie einen Gerätestatus auswählen: *OK*, *Kritisch* oder *Warnung*.

- **Beschreibung des Gerätestatus**

  In diesem Feld können Sie die Kontrollkästchen für jene Bedingungen aktivieren, auf deren Basis einem Gerät eine der folgenden Statusvarianten zugewiesen werden soll: *OK, Kritisch* oder *Warnung*.

- **Vom Programm bestimmter Gerätestatus**

  In dieser Dropdown-Liste können Sie den Wert für den Status des Echtzeitschutzes auswählen. Geräte mit dem angegebenen Echtzeitschutz-Status werden in die Auswahl aufgenommen.

Schutzkomponenten

Im Abschnitt **Schutzkomponenten** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand des Schutzstatus anpassen:

- **Veröffentlichung der Datenbanken**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Veröffentlichungsdatum der Antiviren-Datenbanken. In den Eingabefeldern können Sie den Zeitraum festlegen, anhand dessen die Suche ausgeführt werden soll.

  Diese Option ist standardmäßig deaktiviert.

- **Letzte Virensuche**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Zeitpunkt der letzten Schadsoftware-Untersuchung. In den Eingabefeldern können Sie den Zeitraum festlegen, in dem die Schadsoftware-Untersuchung zum letzten Mal erfolgte.

  Diese Option ist standardmäßig deaktiviert.

- **Gesamtzahl der gefundenen Bedrohungen**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach der Anzahl der gefundenen Viren. In den Eingabefeldern können Sie den unteren und oberen Wert für die Anzahl der gefundenen Viren festlegen.

  Diese Option ist standardmäßig deaktiviert.

Programm-Registry

Auf der Registerkarte **Programm-Registry** können Sie die Kriterien für die Aufnahme von Geräten anhand von installierten Programmen anpassen:

- **Programmname**

  In dieser Dropdown-Liste können Sie einen Anwendungsnamen auswählen. Die Geräte, auf denen diese Anwendung installiert ist, werden in die Auswahl aufgenommen.

- **Programmversion**

  Geben Sie in diesem Eingabefeld die Version der ausgewählten Anwendung ein.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Hersteller der auf dem Gerät installierten Anwendung auswählen.

- **Programm-Status**

  Dropdown-Liste, in der Sie den Status der Anwendung auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen die angegebene Anwendung abhängig vom ausgewählten Status installiert bzw. nicht installiert ist, werden in die Auswahl aufgenommen.

- **Nach Update suchen**

  Wenn diese Option aktiviert ist, erfolgt die Suche anhand der Updatedaten der auf den Geräten installierten Anwendungen. Nachdem Sie das Kontrollkästchen aktiviert haben, ändern sich die Felder **Programmname**, **Programmversion** und **Programm-Status** in **Update-Name**, **Update-Version** und **Status**.

  Diese Option ist standardmäßig deaktiviert.

- **Name der inkompatiblen Sicherheitsanwendung**

  In dieser Dropdown-Liste können Sie Sicherheitsanwendungen von Drittherstellern auswählen. Bei der Suche werden Geräte in die Auswahl aufgenommen, auf denen die ausgewählte Anwendung installiert wurde.

- **Programm-Tag**

  In dieser Dropdown-Liste können Sie ein Anwendungs-Tag auswählen. Alle Geräte, auf denen Programme installiert sind, die den ausgewählten Tag in der Beschreibung haben, werden in die Geräteauswahl aufgenommen.

- **Auf Geräte ohne angegebene Tags anwenden**

  Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in die Auswahl aufgenommen.

  Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

  Diese Option ist standardmäßig deaktiviert.

Hardware-Register

Im Abschnitt **Hardware-Register** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der auf ihnen installierten Hardware anpassen:

- **Gerät**

  In dieser Dropdown-Liste können Sie einen Einheitentyp auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Namen eines Herstellers der Einheit auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- **Gerätename**

  Name des Geräts im Windows-Netzwerk. Ein Gerät mit dem angegebenen Namen wird in die Auswahl aufgenommen.

- **Beschreibung**

  Beschreibung des Geräts oder der Hardware. Geräte mit der in diesem Feld angegebenen Beschreibung werden in die Auswahl aufgenommen.

  Eine Beschreibung in beliebiger Form kann im Fenster Geräteeigenschaften eingegeben werden. Im Feld wird die Volltextsuche unterstützt.

- **Gerätehersteller**

  Bezeichnung des Geräteherstellers. Geräte, die vom angegebenen Hersteller produziert wurden, werden in die Auswahl aufgenommen.

  Der Name des Herstellers kann im Fenster Geräteeigenschaften eingegeben werden.

- **Seriennummer**

  Hardware mit in diesem Feld angegebener Seriennummer wird in die Auswahl aufgenommen.

- **Inventarnummer**

  Hardware mit in diesem Feld angegebener Inventarnummer wird in die Auswahl aufgenommen.

- **Benutzer**

  Hardware des in diesem Feld angegebenen Benutzers wird in die Auswahl aufgenommen.

- **Ort**

  Standort des Geräts bzw. der Hardware (z. B. im Büro oder in der Filiale). Computer oder andere Geräte am in diesem Feld angegebenen Ort werden in die Auswahl aufgenommen.

  Der Ort der Hardware kann in beliebiger Form im Hardware-Eigenschaftenfenster eingegeben werden.

- **Prozessorfrequenz in MHz**

  Frequenzbereich des Prozessors. Geräte mit Prozessoren, die dem Frequenzbereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Virtuelle Prozessorkerne**

  Bereich der Anzahl von virtuellen Cores des Prozessors. Geräte mit Prozessoren, die dem Bereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB)**

  Bereich der Festplattengröße des Geräts. Geräte mit Festplatten, die dem Bereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Speichergröße (MB)**

  Größenbereich des Arbeitsspeichers des Geräts. Geräte mit einem Arbeitsspeicher, der dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

Virtuelle Maschinen

Auf der Registerkarte **Virtuelle Maschinen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anpassen, je nachdem, ob diese Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- **Dies ist eine virtuelle Maschine**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Unwichtig**.
  - **Nein**. Die gesuchten Geräte dürfen keine virtuellen Maschinen sein.
  - **Ja**. Die gesuchten Geräte müssen virtuelle Maschinen sein.

- **Typ der virtuellen Maschine**

  In der Dropdown-Liste können Sie den Hersteller der virtuellen Maschine auswählen.

  Die Dropdown-Liste ist verfügbar, wenn die Werte **Ja** oder **Unwichtig** in der Dropdown-Liste **Dies ist eine virtuelle Maschine** gewählt wurden.

- **Teil einer Virtual Desktop Infrastructure (VDI)**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Unwichtig**.
  - **Nein**. Die gesuchten Geräte dürfen kein Teil der Virtual Desktop Infrastructure (VDI) sein.
  - **Ja**. Die gesuchten Geräte müssen Teil der Virtual Desktop Infrastructure (VDI) sein.

Schwachstellen und Updates

Im Abschnitt **Schwachstellen und Updates** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Quelle der Windows-Updates anpassen:

WUA wurde auf den Administrationsserver umgeschaltet

In dieser Dropdown-Liste können Sie eine der folgenden Varianten der Suche auswählen:

- **Ja**. Bei Auswahl dieser Option werden Geräte in die Suchergebnisse aufgenommen, die Windows-Updates vom Administrationsserver herunterladen.
- **Nein**. Bei Auswahl dieser Option werden Geräte in die Ergebnisse aufgenommen, die Windows-Updates von einer anderen Quelle herunterladen.

Benutzer

Auf der Registerkarte **Benutzer** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Benutzerkonten anpassen, die sich am Betriebssystem angemeldet haben.

- **Letzter am System angemeldeter Benutzer**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer als Letzter angemeldet hat.

- **Benutzer, der sich mindestens einmal am System angemeldet hat**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer mindestens einmal im System angemeldet hat.

Statusbeeinflussende Probleme in verwalteten Programmen

Im Abschnitt **Statusbeeinflussende Probleme in verwalteten Programmen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Liste von möglichen von einem verwalteten Programm gefundenen Problemen anpassen. Wenn zumindest ein ausgewähltes Problem auf einem Gerät existiert, wird das Gerät in die Auswahl aufgenommen. Wenn Sie ein Problem auswählen, das für mehrere Programme aufgelistet ist, haben Sie die Möglichkeit, dieses Problem in allen Listen automatisch auszuwählen.

Beschreibung des Gerätestatus

Sie können die Kontrollkästchen für die Beschreibung der Status der verwalteten Programme aktivieren, bei deren Empfang die Geräte in die Auswahl aufgenommen werden. Wenn Sie einen Status auswählen, der für mehrere Programme aufgelistet ist, haben Sie die Möglichkeit, diesen Status in allen Listen automatisch auszuwählen.

Status der Komponenten in verwalteten Programmen

Im Abschnitt **Status der Komponenten in verwalteten Programmen** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status der Komponenten der verwalteten Programme anpassen:

- **Status des Schutzes vor Datenverlust**

  Suche nach Geräten anhand des Status des "Schutzes vor Datenverlust" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Status des Schutzes der Server für die Zusammenarbeit**

  Suche nach Geräten anhand des Status der Komponente "Schutz der Serverzusammenarbeit" (*Unbekannt*, *Beendet*, *Wird gestartet, Angehalten*, *Wird ausgeführt*, *Fehlgeschlagen*).

- **Status des Antiviren-Schutzes von Mail-Servern**

  Suche nach Geräten anhand des Status des Mail-Server-Schutzes (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Status der Komponente "Endpoint Sensor"**

  Suche nach Geräten anhand des Status der Komponente "Endpoint Sensor" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

Verschlüsselung

Verschlüsselungsalgorithmus

Standard des symmetrischen Algorithmus der Blockverschlüsselung Advanced Encryption Standard (AES). In der Dropdown-Liste können Sie die Länge des Chiffrierschlüssels (56 Bit, 128 Bit, 192 Bit oder 256 Bit) auswählen.

AES56, *AES128*, *AES192*, *AES256*.

Cloud-Segmente

Im Abschnitt **Cloud-Segmente** können Sie die Kriterien für die Aufnahme von Geräten in eine Auswahl anhand ihrer jeweiligen Cloud-Segmente anpassen:

- **Gerät befindet sich in einem Cloud-Segment**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Segment für die Suche auswählen.

  Ist die Option **Inklusive untergeordneter Untergeordnete Objekte einschließen** ebenfalls aktiviert, so wird in allen untergeordneten Objekten des angegebenen Segments eine Suche durchgeführt.

  In die Suchergebnisse werden nur Geräte aus dem ausgewählten Segment aufgenommen.

- **Gerät mithilfe von der API erkannt**

  In der Dropdown-Liste können Sie wählen, ob das Gerät über API gefunden werden soll:

  - **AWS**. Das Gerät wird mithilfe der AWS-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von AWS.
  - **Azure**. Das Gerät wird mithilfe der Azure-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Azure.
  - **Google Cloud.** Das Gerät wird mithilfe der Google-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Google.
  - **Nein**. Das Gerät wird nicht mithilfe der AWS-, Azure- oder Google-API gefunden. Das heißt, es befindet sich entweder außerhalb der Cloud-Umgebung oder es befindet sich in der Cloud-Umgebung, ist aber für die Suche mithilfe API nicht auffindbar.
  - **Kein Wert**. Diese Bedingung trifft nicht zu.

Programmkomponenten

Dieser Abschnitt enthält die Liste der Komponenten jener Anwendungen, in denen entsprechende Verwaltungs-Plug-ins in der Verwaltungskonsole installiert sind.

Im Abschnitt **Programmkomponenten** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status und Versionsnummern der Komponenten festlegen, die sich auf die ausgewählte Anwendung beziehen:

- **Status**

  Suche nach Geräten anhand des Status der Komponente, der von einer Anwendung an den Administrationsserver gesendet wurde. Sie können einen der folgenden Status auswählen: *Keine Daten des Geräts verfügbar*, *Beendet*, *Wird gestartet*, *Angehalten*, *Wird ausgeführt*, *Fehler* oder *Nicht installiert*. Wenn die ausgewählte Komponente der auf einem verwalteten Gerät installierten Anwendung den angegebenen Status aufweist, wird das Gerät bei der Geräteauswahl berücksichtigt.

  Von Anwendungen gesendete Status:

  - *Start*—Die Komponente wird gerade initialisiert.
  - *Wird ausgeführt*–Die Komponente ist aktiviert und funktioniert ordnungsgemäß.
  - *Angehalten*–Die Komponente wird angehalten, z. B. nachdem der Benutzer den Schutz in der verwalteten Anwendung angehalten hat.
  - *Fehler*–Während des Betriebs der Komponente ist ein Fehler aufgetreten.
  - *Beendet*–Die Komponente ist deaktiviert und funktioniert momentan nicht.
  - *Nicht installiert*–Der Benutzer hat die Komponente während der Konfiguration der benutzerdefinierten Installation der Anwendung nicht für die Installation ausgewählt.

  Im Gegensatz zu anderen Status wird der Status *Keine Daten des Geräts verfügbar* nicht von Programmen versendet. Diese Option zeigt, dass die Programme über keine Informationen über den ausgewählten Status der Komponente aufweisen. Dies kann beispielsweise der Fall sein, wenn die ausgewählte Komponente zu keiner der auf dem Gerät installierten Anwendungen gehört oder wenn das Gerät ausgeschaltet ist.

- **Version**

  Suche nach Geräten anhand der Versionsnummer der in der Liste ausgewählten Komponente. Sie können eine Versionsnummer eingeben, beispielsweise `3.4.1.0`, und dann festlegen, ob die ausgewählte Komponente eine gleich, frühere oder spätere Version aufweisen muss. Sie können auch eine Suche nach allen Versionen mit Ausnahme der angegebenen anpassen.

Einstellungen einer Geräteauswahl in eine Datei exportieren

Um die Einstellungen einer Geräteauswahl in eine Datei zu exportieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Klicken Sie im Arbeitsbereich auf die Registerkarte **Auswahl** auf die passende Geräteauswahl in der Liste der benutzerdefinierten Auswahlen.

   Es können nur Einstellungen von Geräteauswahlen, die durch einen Nutzer angelegt wurden, exportiert werden.

3. Klicken Sie auf die Schaltfläche **Auswahl starten**.
4. Klicken Sie auf der Registerkarte **Ergebnisse der Auswahl** auf die Schaltfläche **Einstellungen exportieren**.
5. Geben Sie im folgenden Fenster **Speichern unter** den Namen für die Exportdatei der Auswahleinstellungen ein, geben Sie einen Ordner an, in dem die Datei gespeichert werden soll, und klicken Sie auf die Schaltfläche **Speichern**.

Die Einstellungen der Geräteauswahl werden in der angegebenen Datei gespeichert.

Geräteauswahl erstellen

Um eine Geräteauswahl zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Klicken Sie im Arbeitsbereich des Ordners auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Auswahl erstellen**.
3. Geben Sie im folgenden Fenster **Neue Geräteauswahl** den Namen der zu erstellenden Auswahl an, und klicken Sie auf **OK**.

Daraufhin wird in der Konsolenstruktur im Ordner **Geräteauswahlen** ein neuer Ordner mit dem angegebenen Namen angelegt. Die erstellte Geräteauswahl enthält standardmäßig alle Geräte, die zu den Administrationsgruppen des Administrationsservers gehören, der die Auswahl verwaltet. Damit bestimmte Geräte in der Auswahl angezeigt werden, konfigurieren Sie mithilfe der Schaltfläche **Auswahleigenschaften** die Einstellungen der Auswahl.

Geräteauswahl mit importierten Einstellungen erstellen

Um eine Geräteauswahl anhand der importierten Einstellungen zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Klicken Sie im Arbeitsbereich des Ordners auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Auswahl aus Datei importieren**.
3. Geben Sie im folgenden Fenster den Pfad der Datei an, aus der die Auswahleinstellungen importiert werden sollen Klicken Sie auf **Öffnen**.

Ein Eintrag **Neue Auswahl** wird im Ordner **Geräteauswahlen** angelegt. Die Einstellungen der neuen Auswahl werden aus der Datei importiert, die Sie angegeben haben.

Wenn im Ordner **Geräteauswahlen** eine Auswahl mit dem Namen **Neue Auswahl** bereits vorhanden ist, wird dem Namen der erstellten Auswahl eine Endung der Form **(<laufende Nummer>)** angehängt. Beispiel: **(1)**, **(2)**.

Geräte in der Auswahl aus Administrationsgruppen löschen

Bei der Arbeit mit einer Geräteauswahl können Sie Geräte direkt in der Auswahl aus den Administrationsgruppen löschen, ohne auf die Administrationsgruppen zu wechseln, aus denen die Geräte gelöscht werden sollen.

Um Geräte aus Administrationsgruppen zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Wählen Sie die Geräte aus, die gelöscht werden sollen. Drücken Sie dazu die Taste **Umschalt** oder **Strg**.
3. Löschen Sie die gewählten Geräte aus den Administrationsgruppen auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf eines der gewählten Geräte und wählen Sie **Löschen** aus.
   - Klicken Sie auf die Schaltfläche **Aktion ausführen** und wählen Sie **Aus der Gruppe löschen** in der Dropdown-Liste.

Daraufhin werden die gewählten Geräte aus den Administrationsgruppen gelöscht, zu denen sie gehörten.

Überwachung der Installation und Deinstallation von Anwendungen

Auf verwalteten Geräten können Sie die Installation und Deinstallation bestimmter Anwendungen (z. B. eines bestimmten Browsers) überwachen. Um diese Funktion zu verwenden, können Sie Anwendungen aus der Anwendungsregistrierung zur Liste der überwachten Anwendungen hinzufügen. Wenn eine überwachte Anwendung installiert oder deinstalliert wird, veröffentlicht der Administrationsagent entsprechende Ereignisse wie z. B. **Überwachtes Programm wurde installiert** oder **Überwachtes Programm wurde deinstalliert**. Sie können diese Ereignisse beispielsweise mithilfe von Ereignisauswahlen oder Berichten überwachen.

Sie können diese Ereignisse nur überwachen, wenn sie in der Administrationsserver-Datenbank gespeichert sind.

Um ein Programm zur Liste der zu überwachenden Anwendungen hinzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Erweitert** → **Programmverwaltung** den Unterordner **Programm-Registry** aus.
2. Klicken Sie über der angezeigten Liste der Programmkategorien die Schaltflächen **Eigenschaftenfenster der Programm-Registry öffnen**.
3. Klicken Sie im sich öffnenden Fenster **Zu überwachende Programme** auf die Schaltfläche **Hinzufügen**.
4. Wählen Sie im folgenden Fenster **Wählen Sie einen Programmnamen aus** aus der Anwendungsregistrierung jene Anwendungen aus, für welche die Installation oder Deinstallation überwacht werden soll.
5. Klicken Sie im Fenster **Wählen Sie einen Programmnamen aus** auf **OK**.

Nachdem Sie die Liste der überwachten Anwendungen angepasst haben und eine überwachte Anwendung auf verwalteten Geräten in Ihrer Organisation installiert oder deinstalliert wurde, können Sie die entsprechenden Ereignisse überprüfen, z. B. mithilfe der Ereignisauswahl Letzte Ereignisse.

Ereignisse der Komponenten von Kaspersky Security Center

Jede Komponente von Kaspersky Security Center hat einen eigenen Satz von Ereignistypen. Dieser Abschnitt enthält eine Liste mit Ereignissen, die auf dem Administrationsserver von Kaspersky Security Center, im Administrationsagenten und im iOS MDM-Server auftreten können. Die Typen der Ereignisse, die in den Kaspersky-Anwendungen auftreten, sind in diesem Abschnitt nicht aufgeführt.

Für jedes Ereignis, das von einer Anwendung generiert werden kann, können Sie in der Anwendungsrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Datenstruktur der Beschreibungen von Ereignistypen

Zu jedem Ereignistyp werden der dargestellte Name, der Identifikator (ID), der alphabetische Code, die Beschreibung und die Standard-Speicherdauer angezeigt.

- **Dargestellter Name des Ereignistyps**. Dieser Text wird in Kaspersky Security Center angezeigt, wenn Sie Ereignisse konfigurieren und wenn diese auftreten.
- **Ereignistyp-ID**. Dieser numerische Code wird verwendet, wenn Sie Ereignisse zwecks Ereignisanalyse mithilfe von Drittanbieter-Tools verarbeiten.
- **Ereignistyp** (alphabetischer Code). Dieser Code wird verwendet, wenn Sie Ereignisse mithilfe der in der Datenbank von Kaspersky Security Center verfügbaren öffentlichen Ansichten durchsuchen und verarbeiten und wenn Ereignisse in ein SIEM-System exportiert werden.
- **Beschreibung**. Dieser Text beschreibt die Situationen, in denen ein Ereignis eintreffen kann, und gibt Hinweise auf weiteres Vorgehen.
- **Standard-Speicherdauer**. Das ist die Anzahl der Tage, die ein Ereignis in der Administrationsserver-Datenbank gespeichert bleibt und in der Liste der Ereignisse auf dem Administrationsserver angezeigt wird. Nach Ablauf dieses Zeitraums wird das Ereignis gelöscht. Wenn als Speicherdauer der Wert 0 angegeben ist, werden solche Ereignisse gefunden, aber nicht in der Liste der Ereignisse auf dem Administrationsserver angezeigt. Wenn Sie angegeben haben, dass solche Ereignisse im Ereignisprotokoll des Betriebssystems gespeichert werden sollen, finden Sie die Ereignisse hier.

  Sie können die Speicherdauer von Ereignissen bearbeiten:

  - Verwaltungskonsole: Speicherdauer für ein Ereignis festlegen
  - Kaspersky Security Center Web Console: Speicherdauer für ein Ereignis festlegen

Andere Daten können die folgenden Felder enthalten:

- **event_id**: eindeutige Nummer des Ereignisses in der Datenbank, automatisch generiert und zugewiesen; nicht zu verwechseln mit **Ereignistyp-ID**.
- **task_id**: ID der Aufgabe, die das Ereignis verursacht hat (falls zutreffend)
- **severity**: eine der folgenden Varianten für die Signifikanz (mit aufsteigender Signifikanz):

  0) ungültige Signifikanz

  1) Informativ

  2) Warnung

  3) Fehler

  4) Kritisch

Ereignisse des Administrationsservers

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsserver beziehen.

Ereignisse des Administrationsservers: Kritisch

Die folgende Tabelle enthält die Ereignistypen des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Kritisch**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Wenn Sie den Port in der Verwaltungskonsole im Eigenschaftenfenster des Administrationsservers angegeben haben, **veröffentlicht Kaspersky Security Center seine Metriken** und kritischen Ereignisse, damit diese im Anschluss vom Überwachungs- und Alarmsystem "Prometheus" abgerufen werden können. Prometheus ruft die Metriken und kritischen Ereignisse ab und generiert anschließend Warnungen für jedes Ereignis.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Lizenzbeschränkung wurde überschritten	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Security Center überprüft einmal täglich, ob Lizenzbeschränkungen überschritten wurden. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten die von einer Lizenz abgedeckten werden, 110% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Auch wenn dieses Ereignis eintritt, werden die Client-Geräte geschützt. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center ermittelt die Regeln zum Generieren von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.	180 Tage
Virenangriff	26 (für Schutz vor bedrohlichen Dateien)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art treten auf, wenn auf mehreren verwalteten Geräten die Anzahl an erkannten schädlichen Objekten den Schwellwert innerhalb eines kurzen Zeitraums überschreitet. Sie können auf dieses Ereignis folgendermaßen reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsservers fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird oder erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführt wird.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Virenangriff	27 (für Schutz vor E-Mail-Bedrohungen)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art treten auf, wenn auf mehreren verwalteten Geräten die Anzahl an erkannten schädlichen Objekten den Schwellwert innerhalb eines kurzen Zeitraums überschreitet. Sie können auf dieses Ereignis folgendermaßen reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsservers fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird oder erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführt wird.	180 Tage
Virenangriff	28 (für Firewall)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art treten auf, wenn auf mehreren verwalteten Geräten die Anzahl an erkannten schädlichen Objekten den Schwellwert innerhalb eines kurzen Zeitraums überschreitet. Sie können auf dieses Ereignis folgendermaßen reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsservers fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird oder erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführt wird.	180 Tage
Das Gerät wird nicht mehr verwaltet	4111	KLSRV_HOST_OUT_CONTROL	Ereignisse dieser Art treten auf, wenn ein verwaltetes Gerät ist im Netzwerk sichtbar ist, es aber über einen bestimmten Zeitraum keine Verbindung zum Administrationsserver hergestellt hat. Finden Sie heraus, warum der Administrationsagent auf diesem Gerät nicht ordnungsgemäß ausgeführt wird. Mögliche Ursachen können Netzwerkprobleme oder das Entfernen des Administrationsagenten von diesem Gerät sein.	180 Tage
Gerätestatus - "Kritisch"	4113	KLSRV_HOST_STATUS_CRITICAL	Ereignisse dieser Art treten auf, wenn einem verwalteten Gerät der Status *Kritisch* zugewiesen wird. Sie können die Bedingungen anpassen, unter denen der Gerätestatus zu *Kritisch* wechselt.	180 Tage
Die Schlüsseldatei wurde der Deny-Liste hinzugefügt	4124	KLSRV_LICENSE_BLACKLISTED	Ereignisse dieser Art treten auf, wenn Kaspersky den von Ihnen verwendeten Aktivierungscode oder die Schlüsseldatei auf die Deny-Liste setzt. Kontaktieren Sie den Technischen Support für weitere Informationen.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Eingeschränkter Funktionsmodus	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ereignisse dieser Art treten auf, wenn Kaspersky Security Center beginnt, mit Grundlegenden Funktionen und ohne Schwachstellen- und Patch-Management sowie ohne Funktionalität "Mobile Geräte verwalten", zu arbeiten. Im Folgenden die Gründe für und geeignete Reaktionen auf das Ereignis: • Die Gültigkeitsdauer der Lizenz ist abgelaufen. Um den vollen Funktionsumfang von Kaspersky Security Center zu nutzen, stellen Sie eine Lizenz bereit (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). • Der Administrationsserver verwaltet mehr Geräte, als in der Lizenz angegeben. Verschieben Sie die Geräte aus der Administrationsgruppe des Administrationsservers in die eines anderen Administrationsserver (wenn das Lizenzlimit des anderen Administrationsservers dies zulässt).	180 Tage
Die Lizenz läuft bald ab	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ereignisse dieser Art treten auf, wenn das Ablaufdatum einer kommerziellen Lizenz näher rückt. Einmal am Tag überprüft Kaspersky Security Center, ob sich das Ablaufdatum der Lizenz nähert. Veröffentlicht werden Ereignisse dieses Typs 30 Tage, 15 Tage, 5 Tage und 1 Tag vor dem Ablaufdatum der Lizenz. Die Anzahl der Tage kann nicht geändert werden. Wird der Administrationsserver an dem entsprechenden Tag vor dem Ablaufdatum der Lizenz deaktiviert, so wird das Ereignis erst am darauf folgenden Tag veröffentlicht. Wenn die kommerzielle Lizenz abläuft, stellt Kaspersky Security Center nur grundlegende Funktionen bereit. Sie können auf dieses Ereignis folgendermaßen reagieren: • Vergewissern Sie sich, dass dem Administrationsserver ein Reserve-Lizenzschlüssel hinzugefügt wurde. • Wenn Sie ein Abonnement verwenden, stellen Sie sicher, dies zu Verlängern. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag bis zum Fälligkeitsdatum an den Dienstleister überwiesen wird.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Zertifikat ist abgelaufen	4132	KLSRV_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn auf mobilen Geräten das Client-Zertifikat abläuft.	180 Tage
Das Zertifikat des Administrationsservers ist abgelaufen.	6129	ServerCertificateExpired	Ereignisse dieser Art treten auf, wenn die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ablaufen. Das abgelaufene Zertifikat muss aktualisiert werden.	180 Tage
Die Modul-Updates der Kaspersky-Anwendung wurden widerrufen	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ereignisse dieser Art treten auf, wenn nahtlose Updates von den Kaspersky-Experten zurückgerufen wurden (für diese Updates wird der Status *Zurückgerufen* angezeigt); zum Beispiel, wenn Updates auf eine neuere Version aktualisiert werden müssen. Dieses Ereignis betrifft Patches für Kaspersky Security Center. Module von Anwendungen, die durch Kaspersky verwaltet werden, sind nicht betroffen. Das Ereignis gibt den Grund an, warum das nahtlose Update nicht installiert wurde.	180 Tage
Audit: Export nach SIEM fehlgeschlagen	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Ereignisse dieser Art treten auf, wenn der Export von Ereignissen in das SIEM-System aufgrund eines Verbindungsfehlers mit dem SIEM-System fehlgeschlagen ist.	180 Tage

Ereignisse des Administrationsservers: Funktionsfehler

Die folgende Tabelle enthält die Ereignistypen des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsservers: Funktionsfehler

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Laufzeitfehler	4125	KLSRV_RUNTIME_ERROR	Ereignisse dieser Art treten bei unbekannten Problemen auf. Dabei handelt es sich meistens um DBMS-Probleme, Netzwerkprobleme und andere Hard- und Softwareprobleme. Informationen zu diesem Ereignis stehen in der Ereignisbeschreibung.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Für eine der lizenzierten Programmgruppen wurde die Beschränkung für die Anzahl von Installationen überschritten	4126	KLSRV_INVLICPROD_EXCEDED	Der Administrationsserver generiert Ereignisse dieser Art periodisch (stündlich). Ereignisse dieser Art treten auf, wenn Sie in Kaspersky Security Center die Lizenzschlüssel von Drittanbieter-Programmen verwalten und wenn die Anzahl der Installationen das Limit überschreitet, das durch den Lizenzschlüssel des Drittanbieter-Programms festgelegt ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie Drittanbieter-Anwendungen von den Geräten, auf denen sie nicht verwendet werden. • Verwenden Sie eine Drittanbieter-Lizenz für mehr Geräte. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktionen der lizenzierten Programmgruppe verwenden. Zur lizenzierten Anwendungsgruppe gehören Drittanbieter-Anwendungen, welche die von Ihnen festgelegten Kriterien erfüllen.	180 Tage
Die Abfrage des Cloud-Segments konnte nicht ausgeführt werden	4143	KLSRV_KLCLOUD_SCAN_ERROR	Ereignisse dieser Art treten auf, wenn das Abfragen eines Netzwerksegments in der Cloud-Umgebung durch den Administrationsserver fehlschlägt. Studieren Sie die Informationen in der Ereignisbeschreibung und reagieren Sie entsprechend.	Wird nicht gespeichert
Kopieren der Updates in den angegebenen Ordner nicht ausgeführt	4123	KLSRV_UPD_REPL_FAIL	Ereignisse dieser Art treten auf, wenn Programm-Updates in einen oder mehrere zusätzlich freigegebene Ordner kopiert werden. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob das Benutzerkonto, das für den Zugriff auf die Ordner verwendet wird, über Berechtigung zum Schreiben verfügt. • Prüfen Sie, ob sich der Benutzername und/oder das Kennwort zu diesen Ordnern geändert haben. • Überprüfen Sie die Internetverbindung, da sie die Ursache des Ereignisses sein kann. Folgen Sie den Anweisungen, um Datenbanken und Software-Module zu aktualisieren.	180 Tage
Kein freier Platz auf dem Datenträger	4107	KLSRV_DISK_FULL	Ereignisse dieser Art treten auf, wenn auf der Festplatte des Geräts, auf dem der Administrationsserver installiert ist, freier Speicherplatz knapp wird. Schaffen Sie freien Speicherplatz.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Kein Zugriff auf freigegebenen Ordner	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ereignisse dieser Art treten auf, wenn der Freigegebene Ordner des Administrationsservers nicht verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Überprüfen Sie, ob der Administrationsserver (auf dem sich der freigegebene Ordner befindet) angeschaltet und erreichbar ist. • Prüfen Sie, ob sich der Benutzername und/oder das Kennwort zu diesem Ordner geändert haben. • Prüfen Sie die Netzwerkverbindung.	180 Tage
Die Administrationsserver-Datenbank ist nicht verfügbar	4109	KLSRV_DATABASE_UNAVAILABLE	Ereignisse dieser Art treten auf, wenn die Administrationsserver-Datenbank nicht verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob der Remote-Server, auf dem SQL Server installiert ist, verfügbar ist. • Schauen Sie in die Protokolle des DBMS, um die Ursache für die Nichtverfügbarkeit der Administrationsserver-Datenbank zu finden. Beispielsweise kann aufgrund von präventiven Wartungsarbeiten der Remote-Server, auf dem SQL Server installiert ist, nicht verfügbar sein.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Kein freier Platz in der Administrationsserver-Datenbank	4110	KLSRV_DATABASE_FULL	Ereignisse dieser Art treten auf, wenn in der Administrationsserver-Datenbank kein freier Speicherplatz mehr vorhanden ist. Der Administrationsserver funktioniert nicht, wenn seine Datenbank die Kapazitätsgrenze erreicht hat und wenn weiteres Speichern in der Datenbank nicht möglich ist. Im Folgenden die Gründe für dieses Ereignis, in Abhängigkeit zu dem DBMS, dass Sie verwenden, sowie geeignete Reaktionen auf dieses Ereignis: • Wenn Sie als DBMS die SQL Server Express Edition verwenden: Konsultieren Sie die Dokumentation von SQL Server Express Edition und suchen Sie nach der Größenbeschränkung der von Ihnen genutzten Version. Wahrscheinlich hat die Ihre Administrationsserver-Datenbank die Größenbeschränkung der Datenbank überschritten. Begrenzung der Anzahl der Ereignisse, die in der Administrationsserver-Datenbank gespeichert werden sollen. In der Datenbank des Administrationsservers befinden sich zu viele Ereignisse, die durch die Komponente "Programmkontrolle" gesendet wurden. Sie können die Einstellungen der Richtlinie in Kaspersky Endpoint Security für Windows, die sich auf die Speicherung von Ereignissen der Programmkontrolle in der Administrationsserver-Datenbank bezieht, ändern. • Wenn Sie ein anderes DBMS als SQL Server Express Edition verwenden: Begrenzen Sie nicht die Anzahl der Ereignisse, die in der Administrationsserver-Datenbank gespeichert werden sollen. Verringern Sie die Liste an Ereignissen, die in der Administrationsserver-Datenbank gespeichert werden sollen. Überprüfen Sie die Informationen zur Auswahl des DBMS.	180 Tage

Ereignisse des Administrationsservers: Warnung

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsservers: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Ein häufiges Ereignis wurde erkannt		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Ereignisse dieser Art treten auf, wenn der Administrationsserver ein häufiges auftretendes Ereignis auf einem verwalteten Gerät erkennt. Weitere Informationen finden Sie im folgenden Abschnitt: Blockieren von häufigen auftretenden Ereignissen.	90 Tage
Lizenzbeschränkung wurde überschritten	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center überprüft einmal täglich, ob Lizenzbeschränkungen überschritten wurden. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten die von einer Lizenz abgedeckten werden, 100% bis 110% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Auch wenn dieses Ereignis eintritt, werden die Client-Geräte geschützt. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center ermittelt die Regeln zum Generieren von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Gerät war lange Zeit im Netzwerk inaktiv	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Ereignisse dieser Art treten auf, wenn ein verwaltetes Gerät für längere Zeit inaktiv erscheint. Dies ist meistens dann der Fall, wenn ein verwaltetes Gerät ausrangiert wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Löschen Sie das Gerät manuell aus der Liste der verwalteten Geräte. • Geben Sie mittels der Verwaltungskonsole oder mittels der Kaspersky Security Center Web Console den Zeitraum an, nach dem das Ereignis **Das Gerät war lange Zeit im Netzwerk inaktiv** erstellt wird. • Geben Sie mittels der Verwaltungskonsole oder mittels der Kaspersky Security Center Web Console den Zeitraum an, nach dem das Gerät automatisch aus der Gruppe entfernt wird.	90 Tage
Konflikt von Gerätenamen	4102	KLSRV_EVENT_HOSTS_CONFLICT	Ereignisse dieser Art treten auf, wenn der Administrationsserver zwei oder mehr verwaltete Geräte als ein Gerät wahrnimmt. Dies ist meistens dann der Fall, wenn ein geklontes Laufwerk für die Bereitstellung auf verwalteten Geräten verwendet wurde, und dabei der Administrationsagent auf einem Referenzgerät nicht in den dedizierten "Laufwerk klonen"-Modus versetzt wurde. Um diesen Fehler zu vermeiden, versetzen Sie den Administrationsagenten auf einem Referenzgerät in den "Laufwerk klonen"-Modus, bevor Sie das Laufwerk des Geräts klonen.	90 Tage
Gerätestatus - "Warnung"	4114	KLSRV_HOST_STATUS_WARNING	Ereignisse dieser Art treten auf, wenn einem verwalteten Gerät der Status *Warnung* zugewiesen wird. Sie können die Bedingungen anpassen, unter denen der Gerätestatus zu *Warnung* wechselt.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Für eine der lizenzierten Programmgruppen wird die Beschränkung für die Anzahl von Installationen bald überschritten	4127	KLSRV_INVLICPROD_FILLED	Ereignisse dieser Art treten auf, wenn die Anzahl der Installationen von Drittanbieter-Programmen, die in einer lizenzierten Programmgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben maximalen zulässigen Werts erreicht. Sie können auf dieses Ereignis folgendermaßen reagieren: • Wenn die Drittanbieter-Anwendung auf einigen verwalteten Geräten nicht verwendet wird, löschen Sie die Anwendung von diesen Geräten. • Wenn Sie erwarten, dass die Anzahl der Installationen der Drittanbieter-Anwendung das Maximum in nächster Zukunft übersteigt, sollten Sie im Vorfeld den Erwerb einer Drittanbieter-Lizenz für eine größere Anzahl an Geräten in Erwägung ziehen. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktionen der lizenzierten Programmgruppe verwenden.	90 Tage
Zertifikat wurde angefordert	4133	KLSRV_CERTIFICATE_REQUESTED	Ereignisse dieser Art treten auf, wenn das automatische Neuausstellen eines Zertifikats für die Funktion "Verwaltung mobiler Geräte" fehlschlägt. Im Folgenden werden die Ursachen für das Ereignis und angebrachte Reaktionen darauf ausgeführt: • Die automatische Neuausstellung wurde für ein Zertifikat initiiert, für das die Option **Zertifikat automatisch neu veröffentlichen, falls möglich** deaktiviert ist. Dies kann aufgrund eines Fehler geschehen, der bei der Erstellung des Zertifikats auftrat. Ein manuelles Neuausstellen des Zertifikats kann notwendig sein. • Wenn Sie eine Integration mit einer Public-Key-Infrastruktur verwenden, kann ein fehlendes Namensattribut des SAM-Benutzerkontos, welches für die PKI-Integration und zum Ausstellen der Zertifikate genutzt wird, die Ursache sein. Überprüfen Sie die Eigenschaften des Benutzerkontos.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Zertifikat wurde entfernt	4134	KLSRV_CERTIFICATE_REMOVED	Ereignisse dieser Art treten auf, wenn ein Administrator ein Zertifikat beliebiger Art (General, Mail, VPN) für die Funktion "Verwaltung mobiler Geräte" entfernt. Nach dem Entfernen eines Zertifikats schlägt für die mobilen Geräte, die über dieses Zertifikat verbunden sind, die Verbindung mit dem Administrationsserver fehl. Dieses Ereignis kann hilfreich sein, wenn es darum geht, Fehlfunktionen im Zusammenhang mit der Verwaltung mobiler Geräte aufzuspüren.	90 Tage
Das Zertifikat läuft ab.	6128	ServerCertificateExpiresSoon	Ereignisse dieser Art treten auf, wenn die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ablaufen. Das abgelaufene Zertifikat muss aktualisiert werden.	90 Tage
Das APNs-Zertifikat ist abgelaufen	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn ein APNs-Zertifikat abläuft. Sie müssen manuell das APNs-Zertifikat erneuern und es auf einem iOS MDM-Server installieren.	Wird nicht gespeichert
Das APNs-Zertifikat läuft bald ab	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Ereignisse dieser Art treten auf, wenn das APNs-Zertifikat in weniger als 14 Tagen abläuft. Wenn das APNs-Zertifikat abläuft, müssen Sie manuell das APNs-Zertifikat erneuern und es auf einem iOS MDM-Server installieren. Es wird empfohlen, dass Sie den Zeitpunkt für das Erneuern des APNs-Zertifikats vor das Ablaufdatum legen.	Wird nicht gespeichert
Die FCM-Nachricht konnten nicht an das mobile Gerät gesendet werden	4138	KLSRV_GCM_DEVICE_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Verwaltung mobiler Geräte" so konfiguriert ist, dass sie Firebase Cloud Messaging (FCM) für die Verbindung verwalteter Geräte mit Android Betriebssystem verwendet, und auf dem FCM-Server das Bearbeiten von empfangenen Administrationsserver-Anfragen fehlschlägt. Dies bedeutet, dass einige der verwalteten mobilen Geräte keine PUSH-Benachrichtigungen empfangen. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend. Weitere Informationen über HTTP-Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte der Dokumentation von Firebase Service (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler").	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
HTTP-Fehler beim Versenden der FCM-Nachricht an den FCM-Server	4139	KLSRV_GCM_HTTP_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Verwaltung mobiler Geräte" so konfiguriert ist, dass sie Firebase Cloud Messaging (FCM) für die Verbindung verwalteter Geräte mit Android Betriebssystem verwendet, und der FCM-Server auf eine Administrationsserver-Anfrage einen anderen HTTP-Code als 200 ("OK") zurück liefert. Im Folgenden werden die Ursachen für das Ereignis und angebrachte Reaktionen darauf ausgeführt: • Probleme mit dem FCM-Server. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend. Weitere Informationen über HTTP-Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte der Dokumentation von Firebase Service (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler"). • Probleme mit dem Proxyserver (wenn Sie einen Proxyserver benutzen). Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend.	90 Tage
Die FCM-Nachricht konnte nicht an den FCM-Server gesendet werden	4140	KLSRV_GCM_GENERAL_ERROR	Ereignisse diese Art treten auf, wenn im Rahmen der Verwendung des Firebase Cloud Messaging HTTP-Protokolls unerwartete Fehler auf dem Administrationsserver auftreten. Studieren Sie die Informationen in der Ereignisbeschreibung und reagieren Sie entsprechend. Wenn Sie selbst keine Lösung für dieses Problem ausmachen können, ist es empfehlenswert den Technischen Support von Kaspersky zu kontaktieren.	90 Tage
Auf der Festplatte ist wenig freier Platz vorhanden	4105	KLSRV_NO_SPACE_ON_VOLUMES	Ereignisse dieser Art treten auf, wenn auf dem Gerät, auf dem der Administrationsserver installiert ist, der Speicherplatz knapp wird. Schaffen Sie freien Speicherplatz.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Wenig freier Platz in der Administrationsserver-Datenbank	4106	KLSRV_NO_SPACE_IN_DATABASE	Ereignisse dieser Art treten auf, wenn der Platz in der Administrationsserver-Datenbank zu knapp ist. Wenn Sie diese Situation nicht lösen, erreicht die Administrationsserver-Datenbank bald ihre Kapazitätsgrenze und der Administrationsserver wird nicht länger funktionieren. Nachfolgend finden Sie die Ursachen für dieses Ereignis in Abhängigkeit vom DBMS, das Sie verwenden, sowie geeignete Reaktionen auf dieses Ereignis. Wenn Sie als DBMS die SQL Server Express Edition verwenden: • Konsultieren Sie die Dokumentation von SQL Server Express Edition und suchen Sie nach der Größenbeschränkung der von Ihnen genutzten Version. Wahrscheinlich wird die Datenbank Ihres Administrationsservers die Größenbeschränkung der Datenbank bald erreichen. • Begrenzung der Anzahl der Ereignisse, die in der Datenbank des Administrationsservers gespeichert werden sollen. • In der Datenbank des Administrationsservers befinden sich zu viele Ereignisse, die durch die Komponente "Programmkontrolle" gesendet wurden. Sie können die Einstellungen der Richtlinie in Kaspersky Endpoint Security für Windows, die sich auf die Speicherung von Ereignissen der Programmkontrolle in der Administrationsserver-Datenbank bezieht, ändern. Wenn Sie ein anderes DBMS als SQL Server Express Edition verwenden: • Begrenzen Sie nicht die Anzahl der Ereignisse, die in der Administrationsserver-Datenbank gespeichert werden sollen. • Reduzieren Sie die Liste an Ereignissen, die in der Administrationsserver-Datenbank gespeichert werden sollen. Überprüfen Sie die Informationen zur Auswahl des DBMS.	90 Tage
Die Verbindung mit dem sekundären Administrationsserver wurde getrennt	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum sekundären Administrationsserver unterbrochen ist. Konsultieren Sie das Kaspersky-Ereignisprotokoll des Geräts, auf dem der sekundäre Administrationsserver installiert ist, und reagieren Sie entsprechend.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Verbindung mit dem primären Administrationsserver wurde getrennt	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum primären Administrationsserver unterbrochen ist. Konsultieren Sie das Kaspersky-Ereignisprotokoll des Geräts, auf dem der primäre Administrationsserver installiert ist, und reagieren Sie entsprechend.	90 Tage
Neue Modul-Updates für Kaspersky-Anwendungen wurden registriert	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Ereignisse dieser Art treten auf, wenn der Administrationsserver für Kaspersky-Software, die auf verwalteten Geräten installiert ist, neue Updates registriert, welche eine Genehmigung für die Installation benötigen. Die Updates können Sie mithilfe der Verwaltungskonsole oder mit der Kaspersky Security Center Web Console akzeptieren oder ablehnen.	90 Tage
Die Maximalanzahl an Ereignissen in der Datenbank wurde überschritten. Es wurde mit dem Löschen von Ereignissen begonnen	4145	KLSRV_EVP_DB_TRUNCATING	Ereignisse dieser Art treten auf, wenn das Löschen älterer Ereignisse aus der Administrationsserver-Datenbank begonnen hat, nachdem die Kapazitätsgrenze der Administrationsserver-Datenbank erreicht wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Ändern Sie die maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind. • Reduzieren Sie die Liste an Ereignissen, die in der Datenbank des Administrationsservers gespeichert werden sollen.	Wird nicht gespeichert
Die Maximalanzahl an Ereignissen in der Datenbank wurde überschritten. Die Ereignisse wurden gelöscht	4146	KLSRV_EVP_DB_TRUNCATED	Ereignisse dieser Art treten auf, wenn ältere Ereignisse aus der Administrationsserver-Datenbank gelöscht wurden, nachdem die Kapazitätsgrenze der Administrationsserver-Datenbank erreicht wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Ändern Sie die zulässige maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind. • Reduzieren Sie die Liste an Ereignissen, die in der Datenbank des Administrationsservers gespeichert werden sollen.	Wird nicht gespeichert
Audit (testweise Verbindung zu SIEM-Server fehlgeschlagen)	5120	KLAUD_EV_SIEM_TEST_FAILED	Ereignisse dieser Art treten auf, wenn eine testweise Verbindung mit dem SIEM-Server fehlgeschlagen ist.	30 Tage
Das automatische Ausstellen des Zertifikats ist fehlgeschlagen		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Dieses Ereignis tritt auf, wenn beim Erstellen eines Client-Zertifikats für ein mobiles Gerät ein Fehler auftritt (ein Gerät unter einem mobilen Protokoll).	90 Tage

Ereignisse des Administrationsservers: Information

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Information**.

Ereignisse des Administrationsservers: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer	Anmerkungen
Der Lizenzschlüssel ist zu über 90% verbraucht	4097	KLSRV_EV_LICENSE_CHECK_90	30 Tage	
Neues Gerät wurde erkannt	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 Tage	
Gerät wurde automatisch zur Gruppe hinzugefügt	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 Tage	
Das Gerät wurde entsprechend einer Regel automatisch verschoben	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 Tage	
Das Gerät wurde aus der Gruppe gelöscht: Lange Zeit im Netzwerk inaktiv	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 Tage	
Die Beschränkung für die Anzahl von Installationen wird für eine der lizenzierten Programmgruppen bald überschritten (mehr als 95% verbraucht)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 Tage	
Es wurden Dateien gefunden, die zur Analyse an Kaspersky gesendet werden	4131	KLSRV_APS_FILE_APPEARED	30 Tage	
Die ID der FCM Instance hat sich auf diesem mobilen Gerät geändert	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 Tage	
Updates wurden erfolgreich in den angegebenen Ordner kopiert	4122	KLSRV_UPD_REPL_OK	30 Tage	
Die Verbindung mit dem sekundären Administrationsserver wurde hergestellt	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 Tage	
Die Verbindung mit dem primären Administrationsserver wurde hergestellt	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 Tage	
Datenbanken wurden aktualisiert	4144	KLSRV_UPD_BASES_UPDATED	30 Tage	
Audit: Verbindung mit dem Administrationsserver wurde hergestellt	4147	KLAUD_EV_SERVERCONNECT	30 Tage	

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer	Anmerkungen
Audit: Objekt wurde modifiziert	4148	KLAUD_EV_OBJECTMODIFY	30 Tage	Dieses Ereignis verfolgt Änderungen in den folgenden Objekten: • Administrationsgruppe • Sicherheitsgruppe • Benutzer • Paket • Aufgabe • Richtlinie • Server • Virtueller Server
Audit: Objektstatus wurde geändert	4150	KLAUD_EV_TASK_STATE_CHANGED	30 Tage	Dieses Ereignis tritt beispielsweise auf, wenn eine Aufgabe mit einem Fehler beendet wurde.
Audit: Gruppeneinstellungen wurden modifiziert	4149	KLAUD_EV_ADMGROUP_CHANGED	30 Tage	
Audit: Die Verbindung mit dem Administrationsserver wurde unterbrochen	4151	KLAUD_EV_SERVERDISCONNECT	30 Tage	
Audit: Objekteigenschaften wurden geändert	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 Tage	Dieses Ereignis verfolgt Änderungen der folgenden Eigenschaften: • Benutzer • Lizenz • Server • Virtueller Server
Audit: Benutzerrechte wurden geändert	4153	KLAUD_EV_OBJECTACLMODIFIED	30 Tage	
Audit: Die Chiffrierschlüssel wurden vom Administrationsserver importiert oder exportiert	5100	KLAUD_EV_DPEKEYSEXPORT	30 Tage	
Audit (testweise Verbindung zu SIEM-Server erfolgreich)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 Tage	Dieses Ereignis tritt auf, wenn eine testweise Verbindung mit dem SIEM-Server erfolgreich war.
Reservezertifikat wurde erstellt		ServerReserveCertificateCreated	30 Tage	Dieses Ereignis tritt auf, wenn das Zertifikat des Administrationsservers erstellt wurde.
Zertifikat wird erneuert		ServerCertificateRenewed	30 Tage	Dieses Ereignis tritt auf, wenn das Zertifikat des Administrationsservers erneuert wurde.
Das Zertifikate wurde erfolgreich automatisch ausgestellt		KLSRV_CERTIFICATE_AUTO_ISSUED	30 Tage	Dieses Ereignis tritt auf, wenn ein Zertifikat für ein mobiles Gerät (Gerät unter einem mobilen Protokoll) erfolgreich erstellt wurde.

Die Ereignisse **Reservezertifikat wurde erstellt**, **Zertifikat wird erneuert** und **Das Zertifikate wurde erfolgreich automatisch ausgestellt** werden nur dann automatisch vom Administrationsserver veröffentlicht und in der Verwaltungskonsole angezeigt, wenn die Vorgänge, die diesen Ereignissen entsprechen, für die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ausgeführt werden.

Ereignisse des Administrationsagenten

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsagenten beziehen.

Ereignisse des Administrationsagenten: Funktionsfehler

Die folgende Tabelle enthält die Ereignistypen des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsagenten: Funktionsfehler

Angezeigter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Fehler bei der Update-Installation	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn das automatische Update und Patchen von Komponenten von Kaspersky Security Center fehlgeschlagen sind. Das Ereignis betrifft nicht die Updates von verwalteten Kaspersky-Anwendungen. Lesen Sie die Ereignisbeschreibung. Ein möglicher Grund für dieses Ereignis ist ein Windows-Problem auf dem Administrationsserver. Wenn die Beschreibung ein Problem in der Windows-Konfiguration erwähnt, beheben Sie dieses Problem.	30 Tage
Installation des Updates für Drittherstellersoftware fehlgeschlagen	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion Schwachstellen- und Patch-Management sowie die Funktion Verwaltung mobiler Geräte verwendet werden, und wenn das Update einer Drittanbieter-Software nicht erfolgreich war. Überprüfen Sie, ob der Link zur Software für Drittanbieter gültig ist. Lesen Sie die Ereignisbeschreibung.	30 Tage

Angezeigter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Installation der Updates von Windows-Update fehlgeschlagen	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn Windows Updates nicht erfolgreich waren. Windows-Updates in der Richtlinie des Administrationsagenten anpassen. Lesen Sie die Ereignisbeschreibung. Suchen Sie in der Microsoft Knowledge Base nach dem Fehler. Wenden Sie sich an den technischen Support von Microsoft, wenn Sie das Problem nicht selbst lösen können.	30 Tage
Benutzerverwaltung: Fehler	7723	KLNAG_EV_USR_MNG_ERR	Ereignis bei einer allgemeinen Warnung.	30 Tage
Das Zurücksetzen der sudoers-Datei auf den Referenzwert ist fehlgeschlagen	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der beim Ersetzen der sudoers-Datei aufgetreten ist.	30 Tage
Die Installation der Root-Zertifikate ist fehlgeschlagen	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der bei der Installation von Zertifikaten aufgetreten ist.	30 Tage
Die Root-Zertifikate konnten nicht gelöscht werden	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der beim Entfernen von Zertifikaten aufgetreten ist.	30 Tage

Ereignisse des Administrationsagenten: Warnung

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsagenten: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Während der Installation des Updates des Software-Moduls wurde eine Warnung zurückgegeben	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 Tage
Installation des Updates für die Drittherstellersoftware wurde mit einer Warnung abgeschlossen	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 Tage
Installation des Updates für Drittherstellersoftware wurde aufgeschoben	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 Tage
Es ist ein Sicherheitsproblem aufgetreten	549	GNRL_EV_APP_INCIDENT_OCCURED	30 Tage
KSN-Proxy wurde gestartet. Überprüfen der KSN-Verfügbarkeit nicht ausgeführt	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 Tage
Benutzerverwaltung: Warnungen	7722	KLNAG_EV_USR_MNG_WRN	30 Tage
Die gefundene sudoers-Datei entspricht nicht dem Referenzwert	7724	KLNAG_EV_SUDOER_DIFFERENT	30 Tage

Ereignisse des Administrationsagenten: Information

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Information**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsagenten: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Update für Software-Module wurde erfolgreich installiert	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 Tage
Installation des Updates des Software-Moduls wurde gestartet	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 Tage
Programm wurde installiert	7703	KLNAG_EV_INV_APP_INSTALLED	30 Tage
Programm wurde deinstalliert	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 Tage
Überwachtes Programm wurde installiert	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 Tage
Überwachtes Programm wurde deinstalliert	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 Tage
Drittherstellerprogramm wurde installiert	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 Tage
Neues Gerät wurde hinzugefügt	7708	KLNAG_EV_DEVICE_ARRIVAL	30 Tage
Gerät wurde entfernt	7709	KLNAG_EV_DEVICE_REMOVE	30 Tage
Neues Gerät wurde erkannt	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 Tage
Gerät wurde autorisiert	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 Tage
Windows Desktopfreigabe: Datei wurde gelesen	7712	KLUSRLOG_EV_FILE_READ	30 Tage
Windows Desktopfreigabe: Datei wurde geändert	7713	KLUSRLOG_EV_FILE_MODIFIED	30 Tage
Windows Desktopfreigabe: Das Programm wurde gestartet	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 Tage
Windows Desktopfreigabe: Gestartet	7715	KLUSRLOG_EV_WDS_BEGIN	30 Tage
Windows Desktopfreigabe: Beendet	7716	KLUSRLOG_EV_WDS_END	30 Tage
Update für Drittherstellersoftware wurde erfolgreich installiert	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 Tage
Installation des Updates von Drittherstellersoftware wurde gestartet	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 Tage
KSN-Proxy wurde gestartet. Überprüfung der KSN-Verfügbarkeit wurde erfolgreich abgeschlossen	7719	KSNPROXY_STARTED_CON_CHK_OK	30 Tage
KSN Proxy wurde angehalten	7720	KSNPROXY_STOPPED	30 Tage

Ereignisse des iOS MDM-Servers

Dieser Abschnitt informiert über die Ereignisse, die sich auf den iOS MDM-Server beziehen.

Ereignisse des iOS MDM-Servers: Funktionsfehler

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center iOS MDM-Servers mit der Signifikanz **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des iOS MDM-Servers: Funktionsfehler

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Die Profilliste konnte nicht angefordert werden	PROFILELIST_COMMAND_FAILED	30 Tage
Das Profil konnte nicht installiert werden	INSTALLPROFILE_COMMAND_FAILED	30 Tage
Das Profil konnte nicht entfernt werden	REMOVEPROFILE_COMMAND_FAILED	30 Tage
Die Liste der Provisioning-Profile konnte nicht angefordert werden	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 Tage
Das Provisioning-Profil konnte nicht installiert werden	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 Tage
Das Provisioning-Profil konnte nicht entfernt werden	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 Tage
Die Liste der digitalen Zertifikate konnte nicht angefordert werden	CERTIFICATELIST_COMMAND_FAILED	30 Tage
Die Liste der installierten Programme konnte nicht angefordert werden	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 Tage
Allgemeine Informationen zum mobilen Gerät konnten nicht angefordert werden	DEVICEINFORMATION_COMMAND_FAILED	30 Tage
Sicherheitsinformationen konnten nicht angefordert werden	SECURITYINFO_COMMAND_FAILED	30 Tage
Das mobile Gerät konnte nicht gesperrt werden	DEVICELOCK_COMMAND_FAILED	30 Tage
Das Kennwort konnte nicht gelöscht werden	CLEARPASSCODE_COMMAND_FAILED	30 Tage
Die Daten des mobilen Geräts konnten nicht gelöscht werden	ERASEDEVICE_COMMAND_FAILED	30 Tage
Die App konnte nicht installiert werden	INSTALLAPPLICATION_COMMAND_FAILED	30 Tage
Der Gutscheincode für die App konnte nicht installiert werden	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 Tage
Die Liste der verwalteten Apps konnte nicht angefordert werden	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 Tage
Die verwaltete App konnte nicht entfernt werden	REMOVEAPPLICATION_COMMAND_FAILED	30 Tage
Die Roaming-Einstellungen wurden abgelehnt	SETROAMINGSETTINGS_COMMAND_FAILED	30 Tage
Bei der Ausführung der App ist ein Fehler aufgetreten	PRODUCT_FAILURE	30 Tage
Das Ergebnis der Befehlsausführung enthält ungültige Daten	MALFORMED_COMMAND	30 Tage
Die Benachrichtigung (Push Notification) konnte nicht gesendet werden	SEND_PUSH_NOTIFICATION_FAILED	30 Tage
Der Befehl konnte nicht gesendet werden	SEND_COMMAND_FAILED	30 Tage
Das Gerät wurde nicht gefunden	DEVICE_NOT_FOUND	30 Tage

Ereignisse des iOS MDM-Servers: Warnung

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center iOS MDM-Servers mit der Signifikanz **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des iOS MDM-Servers: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Es wurde versucht, das gesperrte mobile Gerät anzuschließen	INACTICE_DEVICE_TRY_CONNECTED	30 Tage
Profil wurde entfernt	MDM_PROFILE_WAS_REMOVED	30 Tage
Versuch einer wiederholten Verwendung des Client-Zertifikats	CLIENT_CERT_ALREADY_IN_USE	30 Tage
Inaktives Gerät wurde gefunden	FOUND_INACTIVE_DEVICE	30 Tage
Ein Gutscheincode ist erforderlich	NEED_REDEMPTION_CODE	30 Tage
Profil gehört zu einer Richtlinie, die vom Gerät gelöscht wurde	UMDM_PROFILE_WAS_REMOVED	30 Tage

Ereignisse des iOS MDM-Servers: Information

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center iOS MDM-Servers mit der Signifikanz **Information**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des iOS MDM-Servers: Information

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Das neue mobile Gerät wurde angeschlossen	NEW_DEVICE_CONNECTED	30 Tage
Profilliste wurde erfolgreich angefordert	PROFILELIST_COMMAND_SUCCESSFULL	30 Tage
Das Profil wurde erfolgreich installiert	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 Tage
Das Profil wurde erfolgreich gelöscht	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 Tage
Die Liste der Provisioning-Profile wurde erfolgreich angefordert	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 Tage
Das Provisioning-Profil wurde erfolgreich installiert	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 Tage
Das Provisioning-Profil wurde erfolgreich gelöscht	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 Tage
Liste der digitalen Zertifikate wurde erfolgreich angefordert	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 Tage
Die Liste der installierten Programme wurde erfolgreich angefordert	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 Tage
Allgemeine Informationen zum mobilen Gerät wurden erfolgreich angefordert	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 Tage
Sicherheitsinformationen wurden erfolgreich angefordert	SECURITYINFO_COMMAND_SUCCESSFULL	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Das mobile Gerät wurde erfolgreich gesperrt	DEVICELOCK_COMMAND_SUCCESSFULL	30 Tage
Das Kennwort wurde erfolgreich gelöscht	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 Tage
Die Daten auf dem mobilen Gerät wurden erfolgreich bereinigt	ERASEDEVICE_COMMAND_SUCCESSFULL	30 Tage
App wurde erfolgreich installiert	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 Tage
Gutscheincode für die App wurde erfolgreich installiert	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 Tage
Die Liste der verwalteten Apps wurde erfolgreich angefordert	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 Tage
Die verwaltete App wurde erfolgreich entfernt	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 Tage
Roaming-Einstellungen wurden erfolgreich übernommen	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 Tage

Häufige auftretende Ereignisse blockieren

Dieser Abschnitt enthält Informationen über die Verwaltung blockierter häufig auftretender Ereignisse, über das Freigeben blockierter häufig auftretender Ereignisse und über das Exportieren einer Liste mit häufig auftretenden Ereignissen in eine Datei.

Über das Blockieren von häufig auftretenden Ereignissen

Ein verwaltetes Programm (z. B. Kaspersky Endpoint Security für Windows), das auf einem oder mehreren verwalteten Geräten installiert ist, sendet möglicherweise viele Ereignisse des gleichen Typs an den Administrationsserver. Das Empfangen häufig auftretender Ereignisse kann die Administrationsserver-Datenbank überlasten und führt zum Überschreiben anderer Ereignisse. Der Administrationsserver beginnt, die am häufigsten auftretenden Ereignisse zu blockieren, wenn die Anzahl aller empfangenen Ereignisse den für die Datenbank festgelegten Grenzwert überschreitet.

Der Administrationsserver blockiert den Empfang von häufig auftretenden Ereignissen automatisch. Sie können die häufig auftretenden Ereignisse nicht selbst blockieren und auch nicht festlegen, welche Ereignisse blockiert werden sollen.

Um herauszufinden, ob ein Ereignis blockiert wird, können Sie prüfen, ob das Ereignis im Abschnitt **Blockieren häufiger Ereignisse** des Administrationsservers aufgeführt ist. Wenn das Ereignis blockiert ist, können Sie Folgendes tun:

- Wenn Sie verhindern möchten, dass die Datenbank überschrieben wird, können Sie das Empfangen dieser Ereignistypen weiterhin blockieren.
- Wenn Sie beispielsweise den Grund für das häufige Senden eines Ereignisses an den Administrationsserver ermitteln möchten, können Sie häufig auftretende Ereignisse entsperren und die Ereignisse dieses Typs auf diese Weise weiterhin empfangen.
- Wenn Sie die häufig auftretenden Ereignisse weiterhin so lange empfangen möchten, bis sie wieder blockiert werden, können Sie für die häufig auftretenden Ereignisse die Blockierung entfernen.

Das Blockieren von häufig auftretenden Ereignissen verwalten

Der Administrationsserver blockiert den Empfang von häufig auftretenden Ereignissen automatisch, aber Sie können die Blockade aufheben und häufig auftretende Ereignisse weiterhin empfangen. Sie können außerdem den Empfang häufig auftretender Ereignisse blockieren, deren Blockade Sie zuvor aufgehoben haben.

Um das Blockieren von häufig auftretenden Ereignissen zu verwalten:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.
2. Wechseln Sie im Eigenschaftenfenster des Administrationsservers zum Bereich **Abschnitte** und wählen Sie anschließend **Blockieren häufiger Ereignisse**.
3. In dem Abschnitt **Blockieren häufiger Ereignisse**:
   - Wählen Sie die Option **Ereignistyp** für jene Ereignisse, deren Empfang Sie blockieren möchten.
   - Deaktivieren Sie die Option **Ereignistyp** für jene Ereignisse, die Sie weiterhin empfangen möchten.
4. Klicken Sie auf die Schaltfläche **Anwenden**.
5. Klicken Sie auf die Schaltfläche **OK**.

Der Administrationsserver empfängt die häufig auftretenden Ereignisse, für die Sie die Option **Ereignistyp** abgewählt haben, und er blockiert den Empfang der häufig auftretenden Ereignisse, für die Sie die Option **Ereignistyp** gewählt haben.

Die Blockade von häufig auftretenden Ereignissen aufheben

Sie können die Blockade für häufig auftretende Ereignisse aufheben und diese dadurch solange empfangen, bis der Administrationsserver diese Art von häufig auftretenden Ereignissen erneut blockiert.

Um die Blockade von häufig auftretende Ereignisse aufzuheben:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.
2. Wechseln Sie im Eigenschaftenfenster des Administrationsservers zum Bereich **Abschnitte** und wählen Sie anschließend **Blockieren häufiger Ereignisse**.
3. Klicken Sie im Abschnitt **Blockieren häufiger Ereignisse** auf die Zeile des häufig auftretenden Ereignisses, für das Sie die Blockade aufheben möchten.
4. Klicken Sie auf die Schaltfläche **Löschen**.

Das häufig auftretende Ereignis wird aus der Liste der häufig auftretenden Ereignisse entfernt. Der Administrationsserver empfängt Ereignisse dieses Typs.

Liste mit häufigen auftretenden Ereignissen in eine Datei exportieren

Um eine Liste der häufig auftretenden Ereignisse in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.

2. Wechseln Sie im Eigenschaftenfenster des Administrationsservers zum Bereich **Abschnitte** und wählen Sie anschließend **Blockieren häufiger Ereignisse**.

3. Klicken Sie auf die Schaltfläche **In Datei exportieren**.

4. Geben Sie im neuen Fenster zum **Speichern** den Pfad der Datei an, in der die Liste gespeichert werden soll.

5. Klicken Sie auf **Speichern**.

Alle Datensätze in der Liste mit häufigen auftretenden Ereignissen werden in eine Datei exportiert.

Kontrolle über den Status der virtuellen Maschinen

Der Administrationsserver speichert Informationen über den Status der verwalteten Geräte, wie etwa das Hardware-Register und die Liste der installierten Programme, die Einstellungen der verwalteten Programme sowie Aufgaben und Richtlinien. Ist ein verwaltetes Gerät eine virtuelle Maschine, dann kann der Benutzer dessen Status aus dem vorher erstellten Abbild der virtuellen Maschine (Snapshot) zu jedem Zeitpunkt wiederherstellen. Daraufhin werden die Informationen über den Status der virtuellen Maschine auf dem Administrationsserver nicht mehr aktuell.

Beispielsweise hat der Administrator um 12:00 Uhr auf dem Administrationsserver eine Sicherheitsrichtlinie erstellt, die auf der virtuellen Maschine VM_1 um 12:01 Uhr gestartet wurde. Um 12:30 Uhr hat der Benutzer von VM_1 den Status der virtuellen Maschine geändert, indem er auf ihr einen Snapshot wiederhergestellt hat, der bereits 11:00 Uhr angelegt wurde. Infolgedessen wird die Sicherheitsrichtlinie auf der virtuellen Maschine nicht mehr ausgeführt. Auf dem Administrationsserver werden jedoch die nicht aktuellen Informationen darüber gespeichert, dass die Schutzrichtlinie auf der virtuellen Maschine VM_1 aktiv ist.

Kaspersky Security Center erlaubt Ihnen, Änderungen des Status der virtuellen Maschinen zu überwachen.

Der Administrationsserver erstellt nach jeder Synchronisierung mit dem Gerät eine eindeutige ID, die sowohl auf dem Gerät als auch auf dem Administrationsserver gespeichert wird. Vor dem Beginn der folgenden Synchronisierung vergleicht der Administrationsserver die beiden ID-Werte. Stimmen die ID-Werte nicht überein, betrachtet der Administrationsserver die virtuelle Maschine als eine aus einem Abbild wiederhergestellte. Der Administrationsserver setzt die Richtlinien- bzw. Aufgabeneinstellungen für diese virtuelle Maschine zurück und wendet die aktuellen Richtlinien und Gruppenaufgaben auf sie an.

Status des Antiviren-Schutzes mit Systemregistrierung verfolgen

Um den Status des Antiviren-Schutzes auf einem Client-Gerät zu überwachen und dabei Informationen zu verwenden, die vom Administrationsagenten unter Berücksichtigung des Geräte-Betriebssystems aufgezeichnet wurden:

- Auf Windows-Geräten:

  1. Öffnen Sie die Systemregistrierung des Client-Geräts (z. B. lokal mit dem Befehl "regedit" im Menü **Start** → **Ausführen**).

  2. Rufen Sie den folgenden Abschnitt auf:

     - Für 32-Bit-Systeme:

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - Für 64-Bit-Systeme:

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     In der Systemregistrierung werden Informationen über den Status des Antiviren-Schutzes des Client-Geräts angezeigt.

- Auf Linux-Geräten:

  - Die Informationen befinden sich in separaten Textdateien. Es gibt für jeden Datentyp eine Datei. Speicherort: /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- Auf macOS-Geräten:

  - Die Informationen befinden sich in separaten Textdateien. Es gibt für jeden Datentyp eine Datei. Speicherort: /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

Der Status des Antiviren-Schutzes entspricht den Schlüsselwerten der untenstehenden Tabelle.

Registrierungsschlüssel und ihre möglichen Werte

Schlüssel (Datentyp)	Wert	Beschreibung
`Protection_LastConnected (REG_SZ)`	TT-MM-JJJJ HH-MM-SS	Datum und Uhrzeit (UTC-Format) der letzten Herstellung einer Verbindung mit dem Administrationsserver
`Protection_AdmServer (REG_SZ)`	IP, DNS-Name oder NetBIOS-Name	Name des Administrationsservers, der das Gerät verwaltet
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Versionsnummer des Administrationsagenten, der auf dem Gerät installiert ist
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (patch1; patch2; ...; patchN)	Vollständige Nummer der Version des Administrationsagenten (mit Patches), der auf dem Gerät installiert ist
`Protection_HostId (REG_SZ)`	Geräte-ID	ID-Kennung des Geräts
`Protection_DynamicVM (REG_DWORD)`	0 — nein 1 — ja	Der Administrationsagent wird im dynamischen VDI-Modus installiert.
`Protection_AvInstalled (REG_DWORD)`	0 — nein 1 — ja	Auf dem Gerät ist eine Sicherheitsanwendung installiert.

Schlüssel (Datentyp)	Wert	Beschreibung
`Protection_AvRunning (REG_DWORD)`	0 — nein 1 — ja	Der Echtzeitschutz ist auf dem Gerät aktiviert.
`Protection_HasRtp (REG_DWORD)`	0 — nein 1 — ja	Die Echtzeitschutz-Komponente ist installiert.
`Protection_RtpState (REG_DWORD)`	Echtzeitschutz-Status	
	0	Unbekannt
	1	Deaktiviert
	2	Angehalten
	3	Wird gestartet
	4	Aktiviert
	5	Aktiviert mit hohem Schutzniveau (maximaler Schutz)
	6	Aktiviert mit niedrigem Schutzniveau (maximale Geschwindigkeit)
	7	Aktiviert mit standardmäßigen (empfohlenen) Einstellungen
	8	Aktiviert mit benutzerdefinierten Einstellungen
	9	Absturz
`Protection_LastFscan (REG_SZ)`	TT-MM-JJJJ HH-MM-SS	Datum und Uhrzeit (UTC-Format) der letzten vollständigen Untersuchung
`Protection_BasesDate (REG_SZ)`	TT-MM-JJJJ HH-MM-SS	Erscheinungsdatum und -Uhrzeit (im UTC-Format) der Programm-Datenbanken

Maßnahmen anzeigen und konfigurieren, wenn Geräte als inaktiv angezeigt werden

Wenn Client-Geräte innerhalb einer Gruppe inaktiv sind, können Sie Benachrichtigungen darüber erhalten. Sie können solche Geräte auch automatisch löschen.

Um die Aktionen bei inaktiven Geräten innerhalb einer Gruppe anzuzeigen oder anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Konsolenbaum mit der rechten Maustaste auf den Namen der gewünschten Administrationsgruppe.

2. Wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Administrationsgruppe geöffnet.

3. Wechseln Sie im Fenster **Eigenschaften** zum Abschnitt **Geräte**.

4. Aktivieren oder deaktivieren Sie erforderlichenfalls die folgenden Optionen:

   - **Administrator benachrichtigen, wenn Gerät inaktiv seit mehr als (Tagen)**

     Wenn diese Option aktiviert ist, erhält der Administrator Benachrichtigungen über inaktive Geräte. Sie können das Zeitintervall angeben, nach dem das Ereignis **Gerät zu lange inaktiv im Netzwerk** erstellt wird. Standardmäßig beträgt das Zeitintervall 7 Tage.

     Diese Option ist standardmäßig aktiviert.

- **Gerät aus Gruppe entfernen, wenn Gerät inaktiv seit mehr als (Tagen)**

  Wenn diese Option aktiviert ist, können Sie das Zeitintervall festlegen, nach dem das Geräte automatisch aus der Gruppe gelöscht wird. Standardmäßig beträgt das Zeitintervall 60 Tage.

  Diese Option ist standardmäßig aktiviert.

- **Aus übergeordneter Gruppe erben**

  Die Einstellungen in diesem Abschnitt werden von der übergeordneten Gruppe geerbt, in der das Client-Gerät enthalten ist. Wenn diese Option aktiviert ist, sind die Einstellungen unter **Geräteaktivität im Netzwerk** für alle Änderungen gesperrt.

  Diese Option ist nur verfügbar, wenn die Administrationsgruppe über eine übergeordnete Gruppe verfügt.

  Diese Option ist standardmäßig aktiviert.

- **Vererben für untergeordnete Gruppen erzwingen**

  Die Einstellungswerte werden an untergeordnete Gruppen verteilt, aber in den Eigenschaften der untergeordneten Gruppen sind diese Einstellungen gesperrt.

  Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf die Schaltfläche **OK**.

Ihre Änderungen werden gespeichert und übernommen.

Kaspersky-Mitteilungen deaktivieren

In der Kaspersky Security Center Web Console finden Sie im Abschnitt Mitteilungen von Kaspersky (**Überwachung und Berichterstattung → Mitteilungen von Kaspersky**) Wissenswertes zu Ihrer Version von Kaspersky Security Center und den verwalteten Programmen, die auf den verwalteten Geräten installiert sind. Wenn Sie keine Mitteilungen von Kaspersky erhalten möchten, können Sie diese Funktion deaktivieren.

Die Kaspersky-Mitteilungen enthalten zwei Arten von Informationen: sicherheitsrelevante Mitteilungen und Marketing-Mitteilungen. Sie können jeden Mitteilungstyp getrennt deaktivieren.

Um sicherheitsrelevante Mitteilungen zu deaktivieren:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den Sie die sicherheitsrelevanten Mitteilungen deaktivieren möchten.

2. Drücken Sie die rechte Maustaste und wählen Sie im erscheinenden Kontextmenü **Eigenschaften** aus.

3. Deaktivieren Sie im folgenden Eigenschaftenfenster des Administrationsservers, im Abschnitt **Mitteilungen von Kaspersky** die Option **Aktivieren Sie das Anzeigen der Mitteilungen von Kaspersky in Kaspersky Security Center Web Console**.

4. Klicken Sie auf die Schaltfläche **OK**.

Jetzt sind die Kaspersky-Mitteilungen deaktiviert.

Marketing-Mitteilungen sind standardmäßig deaktiviert. Marketing-Mitteilungen erhalten Sie nur, wenn Sie Kaspersky Security Network (KSN) aktiviert haben. Sie können diese Art von Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

Verteilungspunkte und Verbindungs-Gateways anpassen

Die Struktur der Administrationsgruppen in Kaspersky Security Center erfüllt folgende Funktionen:

- Gültigkeitsbereich der Richtlinien festlegen

  Mithilfe von *Richtlinienprofilen* existiert eine alternative Möglichkeit, um die notwendigen Einstellungen auf den Geräten anzuwenden. In diesem Fall legen Sie den Gültigkeitsbereich der Richtlinien mithilfe von Tags, des Speicherorts der Geräte in den Active Directory-Verzeichnissen, oder der Zugehörigkeit zu den Active Directory-Sicherheitsgruppen fest.

- Gültigkeitsbereich der Gruppenaufgaben festlegen

  Es gibt eine Methode zur Festlegung des Gültigkeitsbereichs der Gruppenaufgaben, die nicht auf der Hierarchie der Administrationsgruppen basiert: die Nutzung von Aufgaben für die Geräteauswahlen und eine Reihe von Geräten.

- Festlegung der Zugriffsrechte auf die Geräte, sowie auf die virtuellen und sekundären Administrationsserver

- Weist Verteilungspunkte zu

Beim Aufbau der Struktur der Administrationsgruppen muss für eine optimale Bestimmung der Verteilungspunkte die Netzwerktopologie des Unternehmens berücksichtigt werden. Die optimale Zuordnung der Verteilungspunkte ermöglicht eine Verringerung des Netzwerkverkehrs innerhalb des Unternehmensnetzwerks.

Abhängig von der planmäßigen Struktur des Unternehmens und der Topologie der Netzwerke können die folgenden typischen Konfigurationen für die Struktur der Administrationsgruppen unterschieden werden:

- Einzelbüro

- Mehrere kleine, eigenständige Büros

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Typische Konfiguration von Verteilungspunkten: Einzelbüro

In einer typischen Einzelbüro-Konfiguration befinden sich alle Geräte im Netzwerk des Unternehmens und können einander "sehen". Das Netzwerk des Unternehmens kann aus mehreren ausgewählten Teilen (der Netzwerke oder der Netzwerksegmente) bestehen, die über enge Kanäle verbunden sind.

Es sind die folgenden Methoden für den Aufbau der Struktur der Administrationsgruppen möglich:

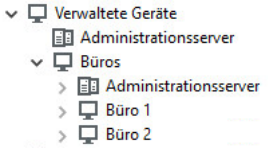
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen. Die Verteilungspunkte können automatisch bestimmt oder manuell zugewiesen werden.

- Aufbau der Struktur der Administrationsgruppen, in der die Netztopologie nicht widergespiegelt wird. In diesem Fall müssen Sie die automatische Bestimmung der Verteilungspunkte deaktivieren und dann für die Stammadministrationsgruppe in jedem ausgewählten Teil des Netzwerkes ein oder mehrere Geräte als Verteilungspunkte bestimmen, beispielsweise für die Gruppe **Verwaltete Geräte**. Alle Verteilungspunkte befinden sich dann auf einer Ebene und haben den identischen Gültigkeitsbereich, der alle Geräte im Netzwerk des Unternehmens umfasst. Jeder Administrationsagent wird in diesem Fall mit dem Verteilungspunkt verbunden, zu dem die Route am kürzesten ist. Die Route zum Verteilungspunkt kann mithilfe des Tools "tracert" bestimmt werden.

Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros

Diese typische Konfiguration entspricht einer Menge kleiner Remote-Büros, die eventuell durch das Internet mit dem Hauptbüro verbunden sind. Jedes der Remote-Büros befindet sich hinter einer NAT. Das bedeutet, dass ein Remote-Büro nicht mit einem anderen verbunden werden kann und die Büros voneinander isoliert sind.

Diese Konfiguration muss in der Struktur der Administrationsgruppen widergespiegelt werden: für jedes Remote-Büro muss eine separate Administrationsgruppe erstellt werden (entspr. Gruppen **Büro 1**, **Büro 2** auf der nachfolgenden Abbildung).



Die Remote-Büros werden in der Struktur der Administrationsgruppen abgebildet.

Für jede Administrationsgruppe, die einem Büro entspricht, müssen ein oder mehrere Verteilungspunkte festgelegt werden. Als Verteilungspunkte müssen Geräte des Remote-Büros bestimmt werden, die genug freien Platz auf dem Datenträger haben. Die Geräte, die sich beispielsweise in der Gruppe **Büro 1** befinden, wenden sich an die Verteilungspunkte, die für die Administrationsgruppe **Büro 1** bestimmt wurden.

Wenn einige Benutzer samt ihren Laptops physisch zwischen Büros wechseln, müssen in jedem Remote-Büro zusätzlich zu den oben erwähnten Verteilungspunkten zwei oder mehrere Geräte ausgewählt und als Verteilungspunkte für die Administrationsgruppe der obersten Ebene bestimmt werden (Gruppe **Stammgruppe für die Büros** in der obigen Abbildung).

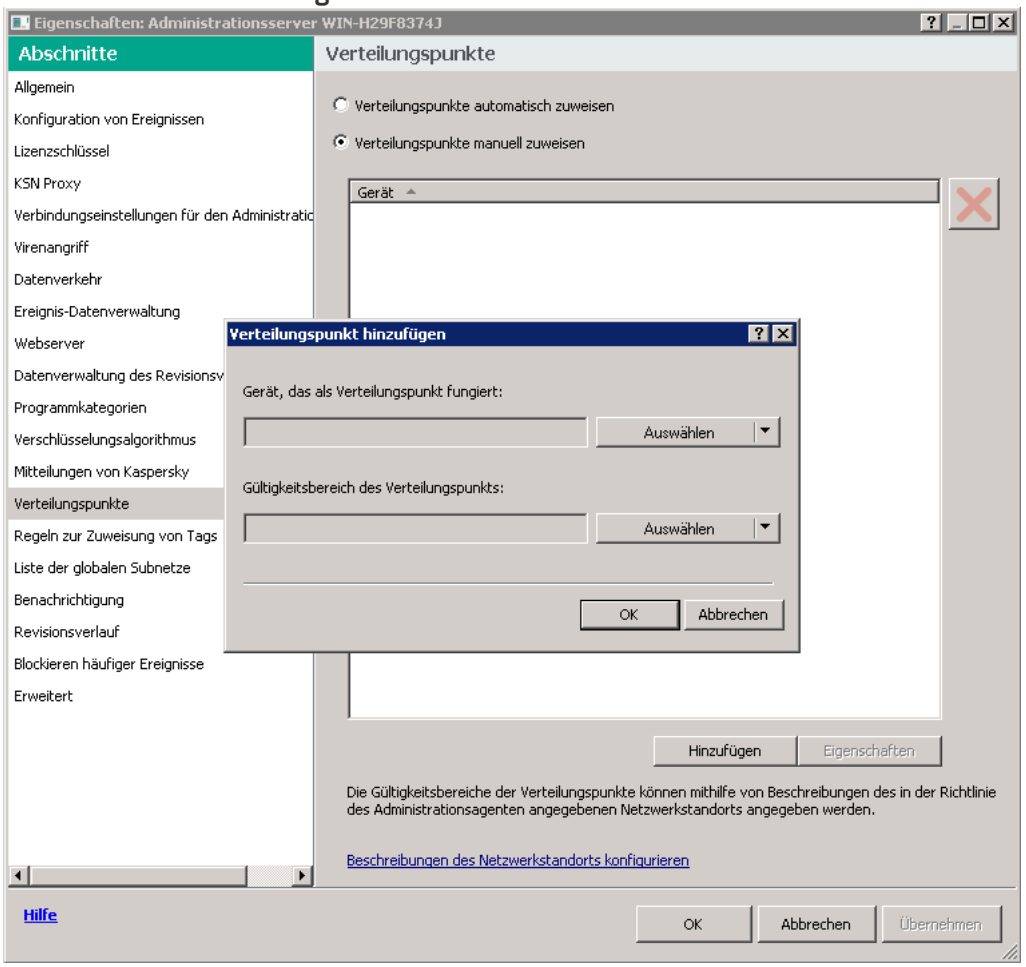
Beispiel: Es gibt einen Laptop, der sich in der Administrationsgruppe **Büro 1** befindet, aber physisch in ein Büro gebracht wird, das der Gruppe **Büro 2** entspricht. Nach dem Ortswechsel versucht der Administrationsagent auf dem Laptop, sich an die Verteilungspunkte zu wenden, die zur Gruppe **Büro 1** gehören. Diese Verteilungspunkte erweisen sich allerdings als nicht verfügbar. Dann beginnt der Administrationsagent, sich an die Verteilungspunkte zu wenden, die für die Gruppe **Stammgruppe für die Büros** bestimmt wurden. Da die Remote-Büros voneinander isoliert sind, werden von allen Verteilungspunkten, die für die Administrationsgruppe **Stammgruppe für die Büros** bestimmt wurden, nur die Zugriffe des Administrationsagenten auf die Verteilungspunkte erfolgreich sein, die für die Gruppe **Büro 2** bestimmt wurden. Das bedeutet, dass der Laptop zwar in der Administrationsgruppe bleibt, die dem ursprünglichen Büro entspricht, aber die Verteilungspunkte jenes Büros verwendet, in dem er sich in diesen Moment physisch befindet.

Zuweisen eines verwalteten Geräts als Verteilungspunkt

Sie können ein Gerät manuell als Verteilungspunkt für die Administrationsgruppe festlegen und in der Verwaltungskonsole als Verbindungs-Gateway konfigurieren.

Um ein Gerät zum Verteilungspunkt der Administrationsgruppe zu bestimmen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Verteilungspunkte** aus.
4. Wählen Sie im rechten Teil des Fensters die Option **Verteilungspunkte manuell zuweisen**.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.



Einen Verteilungspunkt manuell zuweisen

Das Fenster **Verteilungspunkt hinzufügen** wird geöffnet.

6. Gehen Sie im Fenster **Verteilungspunkt hinzufügen** wie folgt vor:

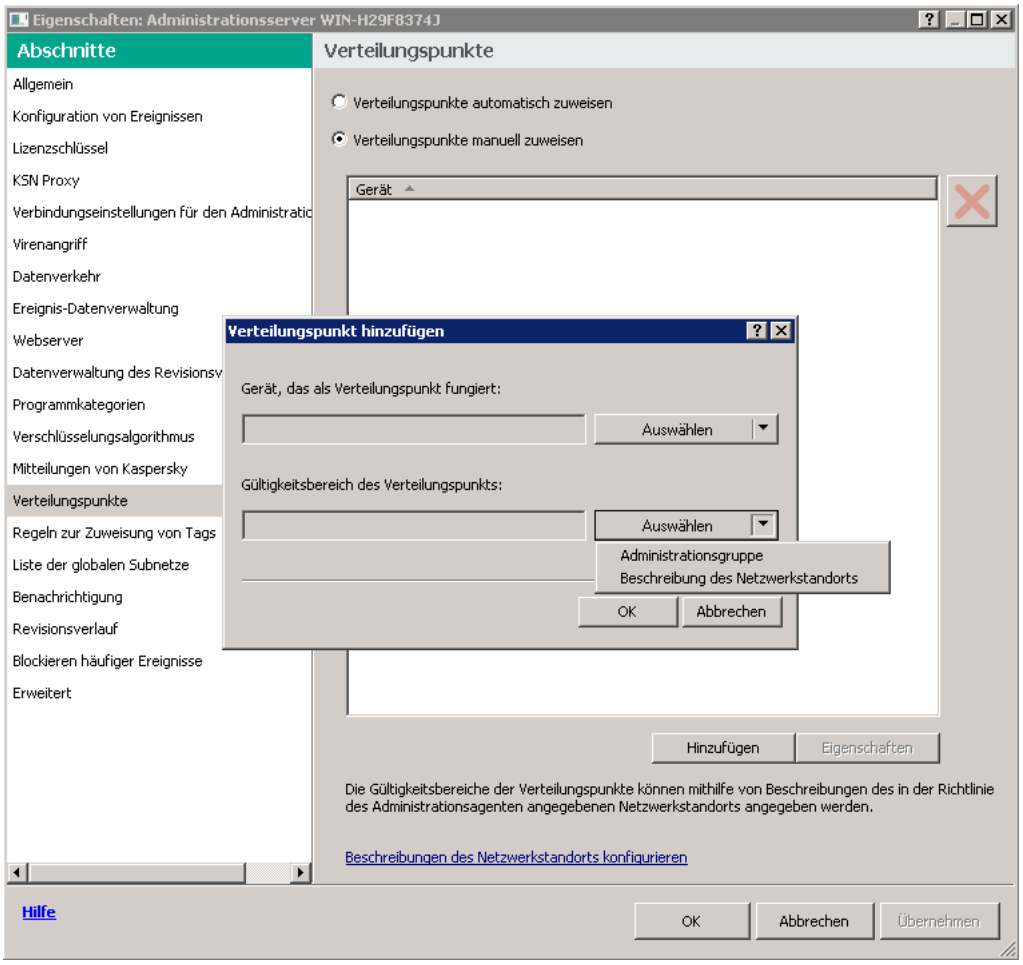
   a. Klicken Sie unter **Gerät, welches als Verteilungspunkt fungieren soll** auf den Abwärtspfeil der geteilten Schaltfläche **Auswählen** und wählen Sie die Option **Gerät aus der Gruppe hinzufügen** aus.

   b. Wählen Sie im neuen Fenster **Geräte auswählen** das Gerät aus, welches als Verteilungspunkt fungieren soll.

c. Klicken Sie unter **Bereich des Verteilungspunkts** auf den Abwärtspfeil der geteilten Schaltfläche **Auswählen**.

d. Geben Sie eine Reihe von Geräten an, an die der Verteilungspunkt Updates verteilen soll. Sie können eine Administrationsgruppe oder eine Beschreibung des Netzwerkspeicherorts angeben.

e. Klicken Sie auf **OK**, um das Fenster **Verteilungspunkt hinzufügen** zu schließen.



Auswählen des Gültigkeitsbereichs des Verteilungspunkts

Der hinzugefügte Verteilungspunkt wird in der Liste der Verteilungspunkte im Abschnitt **Verteilungspunkte** angezeigt.

Das erste Gerät mit installiertem Administrationsagenten, das eine Verbindung zum virtuellen Administrationsserver herstellt, wird automatisch zum Verteilungspunkt bestimmt und als Verbindungs-Gateway konfiguriert.

Verbinden eines Linux-Gerätes als Gateway in einer demilitarisierten Zone

Um ein Linux-Gerät als Gateway in einer demilitarisierten Zone (DMZ) zu verbinden:

1. Laden Sie den Administrationsagenten herunter und installieren Sie den Administrationsagenten auf einem Linux-Gerät.

2. Führen Sie das Post-Installationsskript aus und folgen Sie dem Assistenten, um die lokale Umgebungskonfiguration einzustellen. Führen Sie in der Befehlszeile folgenden Befehl aus:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Wählen Sie in dem Schritt, in dem nach dem Modus des Administrationsagenten gefragt wird, die Option **Als Verbindungs-Gateway verwenden** aus.

4. Wählen Sie in der MMC-basierten Verwaltungskonsole des Administrationsservers den Punkt **Eigenschaften** aus.

5. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers den Abschnitt **Verteilungspunkte** aus.

6. Führen Sie auf der rechten Seite des sich öffnenden Fensters **Verteilungspunkte** Folgendes aus:

   a. Wählen Sie die Option **Manuelle Zuweisung der Verteilungspunkte** aus.

   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Verteilungspunkt hinzufügen** wird geöffnet.

7. Gehen Sie im Fenster **Verteilungspunkt hinzufügen** wie folgt vor:

   a. Klicken Sie unter **Gerät, welches als Verteilungspunkt fungieren soll** auf den Abwärtspfeil der geteilten Schaltfläche **Auswählen** und wählen Sie anschließend die Option **Verbindungs-Gateway in der demilitarisierten Zone nach Adresse hinzufügen** aus.

   b. Klicken Sie unter **Bereich des Verteilungspunkts** auf den Abwärtspfeil der geteilten Schaltfläche **Auswählen**.

   c. Geben Sie eine Reihe von Geräten an, an die der Verteilungspunkt Updates verteilen soll. Sie können eine Administrationsgruppe angeben.

   d. Klicken Sie auf **OK**, um das Fenster **Verteilungspunkt hinzufügen** zu schließen.

8. Der hinzugefügte Verteilungspunkt wird in der Liste der Verteilungspunkte im Abschnitt **Verteilungspunkte** angezeigt.

9. Führen Sie das Tool "klnagchk" aus, um zu prüfen, ob eine erfolgreiche Verbindung zu Kaspersky Security Center konfiguriert wurde. Führen Sie in der Befehlszeile Folgendes aus:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. Wechseln Sie im Hauptmenü zu Kaspersky Security Center und finden Sie das Gerät.

11. Klicken Sie im folgenden Fenster auf <Gerätename>.

12. Wählen Sie in der Dropdown-Liste den Link **In Gruppe verschieben** aus.

13. Klicken Sie in dem sich öffnenden Fenster **Gruppe auswählen** auf den Link **Verteilungspunkte**.

14. Klicken Sie auf die Schaltfläche **OK**.

15. Starten Sie den Dienst des Administrationsagenten auf dem Linux-Gerät durch Ausführen der folgenden Befehlszeileneingabe neu:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

Das Verbinden eines Linux-Gerätes als Gateway in der demilitarisierten Zone ist abgeschlossen.

Anschließend können Sie über das konfigurierte Verbindungs-Gateway ein Linux-Gerät mit dem Administrationsserver verbinden. Führen Sie diese Maßnahmen erst aus, nachdem Sie das Hauptinstallationsszenario abgeschlossen haben.

Verbinden eines Linux-Geräts mit dem Administrationsserver über ein Verbindungs-Gateway

Ein Verbindungs-Gateway ermöglicht es, Client-Geräte aus der demilitarisierten Zone (DMZ) mit dem Administrationsserver zu verbinden. Als Verbindungs-Gateway können Windows- und Linux-basierte Geräte fungieren. Nachdem Sie das Verbindungs-Gateway verbunden und konfiguriert haben, können Sie dieses Gateway verwenden, um ein Linux-Gerät mit dem Administrationsserver zu verbinden. Führen Sie die unten beschriebenen Maßnahmen erst aus, nachdem Sie das Hauptinstallationsszenario abgeschlossen haben.

Führen Sie auf diesem Gerät die folgenden Aktionen aus, um ein Linux-Gerät über ein Verbindungs-Gateway mit dem Administrationsserver zu verbinden:

1. Laden Sie den Administrationsagenten herunter und installieren Sie den Administrationsagenten auf einem Linux-Gerät.

2. Führen Sie das Post-Installationsskript des Administrationsagenten auf dem Linux-Gerät durch Ausführen der folgenden Befehlszeileneingabe aus:
    ```
    $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
    ```

3. Wählen Sie in dem Schritt, in dem nach dem Modus des Administrationsagenten gefragt wird, die Option **Mittels Verbindungs-Gateway mit Server verbinden** aus und geben Sie die Adresse des Verbindungs-Gateways ein.

4. Überprüfen Sie die Verbindung mit Kaspersky Security Center und dem Verbindungs-Gateway unter Verwendung der folgenden Befehlszeileneingabe:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
    ```
    Die Adresse des Verbindungs-Gateways wird in der Ausgabe angezeigt.

Das Verbinden eines Linux-Geräts mit dem Administrationsserver über ein Verbindungs-Gateway ist abgeschlossen. Mit diesem Gerät können Sie die Verteilung aktualisieren, Programme remote-installieren und Informationen zu vernetzten Geräten abrufen.

Hinzufügen eines Verbindungs-Gateways als Verteilungspunkt innerhalb der DMZ

Statt selbst eine Verbindung zum Administrationsserver herzustellen, wartet ein Verbindungs-Gateway auf eine Verbindung vom Administrationsserver. Das bedeutet, dass das Gerät mit dem Verbindungs-Gateway in der DMZ direkt nach der Installation des Verbindungs-Gateways vom Administrationsserver nicht unter den verwalteten Geräten angezeigt wird. Es ist daher eine spezielle Vorgehensweise notwendig, um sicherzustellen, dass der Administrationsserver eine Verbindung zum Verbindungs-Gateway initiiert.

Um ein Gerät mit einem Verbindungs-Gateway als Verteilungspunkt hinzuzufügen:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Verteilungspunkte** aus.
4. Wählen Sie im rechten Teil des Fensters die Option **Verteilungspunkte manuell zuweisen**.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Verteilungspunkt hinzufügen** wird geöffnet.
6. Gehen Sie im Fenster **Verteilungspunkt hinzufügen** wie folgt vor:

   a. Klicken Sie unter **Gerät, welches als Verteilungspunkt fungieren soll** auf den Abwärtspfeil der geteilten Schaltfläche **Auswählen** und wählen Sie anschließend die Option **Verbindungs-Gateway in der demilitarisierten Zone nach Adresse hinzufügen** aus.

   b. Geben Sie im sich öffnenden Fenster **Eingeben der Verbindungs-Gateway-Adresse** die IP-Adresse des Verbindungs-Gateways ein (oder dessen Namen, wenn das Verbindungs-Gateway über den Namen erreichbar ist).

   c. Klicken Sie unter **Bereich des Verteilungspunkts** auf den Abwärtspfeil der geteilten Schaltfläche **Auswählen**.

   d. Geben Sie eine Reihe von Geräten an, an die der Verteilungspunkt Updates verteilen soll. Sie können eine Administrationsgruppe oder eine Beschreibung des Netzwerkspeicherorts angeben.

      Es wird empfohlen, für externe verwaltete Geräte eine separate Gruppe zu führen.

Nachdem Sie diese Vorgänge ausgeführt haben, enthält die Liste der Verteilungspunkte einen neuen Eintrag mit dem Namen **Temporärer Eintrag für Verbindungs-Gateway**.

Nahezu sofort versucht sich der Administrationsserver mit dem Verbindungs-Gateway über die von Ihnen angegebene Adresse zu verbinden. Ist dies erfolgreich, wird der Name des Eintrags in den Namen des Geräts mit dem Verbindungs-Gateway geändert. Dieser Vorgang kann bis zu 5 Minuten dauern.

Während der Konvertierung des temporären Eintrags für den Verbindungs-Gateway in einen benannten Eintrag, wird das Verbindungs-Gateway auch in der Gruppe **Nicht zugeordnete Geräte** angezeigt.

Um ein Verbindungs-Gateway einem bereits konfigurierten Netzwerk hinzuzufügen, installieren Sie den Administrationsagenten auf den Geräten erneut, die Sie mit dem neu hinzugefügten Verbindungs-Gateway verbinden möchten.

Verteilungspunkte automatisch zuweisen

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. Kaspersky Security Center wählt dann selbst aus, welche Geräte zu Verteilungspunkten zugewiesen werden.

Um Verteilungspunkte automatisch zuzuweisen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des Administrationsservers aus, für den Sie Verteilungspunkte automatisch zuweisen möchten.
3. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
4. Wählen Sie im Fenster "Eigenschaften des Administrationsservers" im Bereich **Abschnitte** die Option **Verteilungspunkte** aus.
5. Wählen Sie im rechten Teil des Fensters die Option **Verteilungspunkte automatisch zuweisen**.

   Wenn die automatische Gerätezuweisung für Verteilungspunkte aktiviert ist, können die Einstellungen der Verteilungspunkte nicht manuell angepasst werden und die Liste der Verteilungspunkte kann nicht verändert werden.

6. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin beginnt der Administrationsserver damit, Verteilungspunkte automatisch zu bestimmen und ihre Einstellungen zu konfigurieren.

Administrationsagenten lokal auf dem als Verteilungspunkt ausgewählten Gerät installieren

Damit das Gerät, das als Verteilungspunkt ausgewählt wurde, direkt mit dem virtuellen Administrationsserver verbunden werden kann, um die Rolle des Verbindungs-Gateways zu übernehmen, muss der Administrationsagent lokal auf diesem Gerät installiert werden.

Die Reihenfolge der lokalen Installation des Administrationsagenten auf dem Gerät, das als Verteilungspunkt ausgewählt wurde, stimmt mit der Reihenfolge der lokalen Installation des Administrationsagenten auf jedem Gerät im Netzwerk überein.

Für das Gerät, das als Verteilungspunkt ausgewählt wurde, müssen folgende Bedingungen erfüllt sein:

- Bei der lokalen Installation des Administrationsagenten muss im Fenster des Installationsassistenten **Administrationsserver** im Feld **Serveradresse** die Adresse des virtuellen Administrationsservers angegeben werden, der das Gerät verwaltet. Als Adresse des Geräts können Sie die IP-Adresse oder den Namen des Geräts im Windows-Netzwerk angeben.

  Geben Sie die Adresse des virtuellen Administrationsservers auf folgende Weise an: <Vollständige Adresse des physikalischen Administrationsservers, dem der virtuelle Server untergeordnet ist>/<Name des virtuellen Administrationsservers>.

- Damit das Gerät als Verbindungs-Gateways funktionieren kann, müssen alle Ports auf dem Gerät geöffnet sein, die für die Verbindung mit dem Administrationsserver erforderlich sind.

Aufgrund der Installation des Administrationsagenten mit den vorgegebenen Einstellungen auf dem Gerät führt Kaspersky Security Center automatisch die folgenden Aktionen aus:

- Nimmt das Gerät in die Gruppe **Verwaltete Geräte** des virtuellen Administrationsservers auf.

- Ernennt dieses Gerät zum Verteilungspunkt der Gruppe **Verwaltete Geräte** des virtuellen Administrationsservers.

Es ist erforderlich und ausreichend, den Administrationsagenten lokal auf einem Gerät zu installieren, das zum Verteilungspunkt der Gruppe **Verwaltete Geräte** im Unternehmensnetzwerk ernannt wurde. Sie können den Administrationsagenten von einem entfernten Standort auf jene Geräte installieren, die als Verteilungspunkte in den untergeordneten Administrationsgruppen fungieren. Verwenden Sie dabei den Verteilungspunkt der Gruppe **Verwaltete Geräte** als Verbindungs-Gateway.

Verteilungspunkt als Verbindungs-Gateway verwenden

Wenn der Administrationsserver zur demilitarisierten Zone (DMZ) nicht gehört, ist das Herstellen einer Verbindung zwischen den Administrationsagenten, die zur demilitarisierten Zone gehören, und dem Administrationsserver nicht möglich.

Zum Herstellen einer Verbindung zwischen dem Administrationsserver und den Administrationsagenten kann ein Verteilungspunkt als Verbindungs-Gateway verwendet werden. Der Verteilungspunkt stellt dem Administrationsserver den Port für den Verbindungsaufbau zur Verfügung. Der Administrationsserver stellt beim Starten eine Verbindung zum Verteilungspunkt her und trennt diese Verbindung während seines Betriebs nicht.

Nachdem der Verteilungspunkt ein Signal des Administrationsservers empfangen hat, sendet er ein UDP-Signal an die Administrationsagenten zur Verbindung mit dem Administrationsserver. Nach Empfang des Signals werden die Administrationsagenten mit dem Verteilungspunkt verbunden, der Informationen zwischen den Administrationsagenten und dem Administrationsserver übermittelt. Der Informationsaustausch kann über ein IPv4- oder IPv6-Netzwerk erfolgen.

Es wird empfohlen, ein speziell dazu bestimmtes Gerät als Verbindungs-Gateway zu verwenden und einem einzelnen Gateway maximal 10.000 Client-Geräte (einschließlich mobile Geräte) zuzuweisen.

So fügen Sie einem zuvor konfigurierten Netzwerk ein Verbindungs-Gateway hinzu:

1. Installieren Sie Administrationsagenten Verbindungs-Gateway-Modus.

2. Installieren Sie den Administrationsagenten auf den Geräten erneut, die Sie mit dem neu hinzugefügten Verbindungs-Gateway verbinden möchten.

Weitere IP-Bereiche zur Liste mit Bereichen hinzufügen, die von einem Verteilungspunkt abgefragt werden

Sie können einen IP-Bereich zur Liste der vom Verteilungspunkt abgefragten Bereiche hinzufügen.

So fügen Sie einen IP-Bereich zur Liste der abgefragten Bereiche hinzu:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Kontextmenü des Knotens **Eigenschaften** aus.
3. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers den Abschnitt **Verteilungspunkte** aus.
4. Wählen Sie in der Liste den gewünschten Verteilungspunkt aus und klicken Sie anschließend auf **Eigenschaften**.
5. Wählen Sie in dem sich öffnenden Eigenschaftenfenster des Verteilungspunkts, im linken Bereich von **Abschnitte**, die Option **Gerätesuche → IP-Bereiche** aus.
6. Aktivieren Sie das Kontrollkästchen **Abfrage des Bereichs zulassen**.
7. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Die Schaltfläche **Hinzufügen** ist nur aktiv, wenn Sie das Kontrollkästchen **Abfrage des Bereichs zulassen** aktivieren.

   Das Fenster **IP-Bereich** wird geöffnet.
8. Geben Sie im Fenster **IP-Bereich** den Namen des neuen IP-Bereichs ein (der Standardname lautet "Neuer Bereich").
9. Klicken Sie auf die Schaltfläche **Hinzufügen**.
10. Führen Sie eine der folgenden Aktionen aus:

    - Geben Sie den IP-Bereich mit Start- und End-IP-Adresse ein.
    - Geben Sie den IP-Bereich mit Adresse und Subnetzmaske ein.
    - Klicken Sie auf **Durchsuchen** und fügen Sie ein Subnetz aus der Globalen Liste der Subnetze hinzu.
11. Klicken Sie auf die Schaltfläche **OK**.
12. Klicken Sie auf **OK**, um den neuen Bereich mit dem festgelegten Namen hinzuzufügen.

Der neue Bereich wird in der Liste der abgefragten Bereiche angezeigt.

Verteilungspunkt als Push-Server verwenden

In Kaspersky Security Center kann ein Verteilungspunkt als Push-Server für Geräte fungieren, die über das mobile Protokoll oder über den Administrationsagenten verwaltet werden. Ein Push-Server muss beispielsweise aktiviert sein, wenn Sie die erzwungene Synchronisierung von KasperskyOS-Geräten mit dem Administrationsserver verwenden möchten. Ein Push-Server besitzt denselben Umfang verwalteter Geräte wie der Verteilungspunkt, auf dem der Push-Server aktiviert ist. Wenn Sie mehrere Verteilungspunkte derselben Administrationsgruppe zugewiesen haben, können Sie den Push-Server auf jedem der Verteilungspunkte aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

Ein Push-Server unterstützt die Last von bis zu 50.000 gleichzeitigen Verbindungen.

Möglicherweise möchten Sie Verteilungspunkte als Push-Server verwenden, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht. Für einige Vorgänge ist eine durchgängige Verbindung erforderlich, z. B. das Starten und Stoppen lokaler Aufgaben, das Empfangen von Statistiken für eine verwaltete Anwendung oder die Herstellung eines Tunnels. Wenn Sie einen Verteilungspunkt als Push-Server verwenden, müssen Sie weder die Option **Verbindung mit Administrationsserver nicht trennen** auf verwalteten Geräten verwenden, noch Pakete an den UDP-Port des Administrationsagenten senden.

So verwenden Sie einen Verteilungspunkt als Push-Server:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Kontextmenü des Knotens **Eigenschaften** aus.
3. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers den Abschnitt **Verteilungspunkte** aus.
4. Wählen Sie in der Liste den gewünschten Verteilungspunkt aus und klicken Sie anschließend auf **Eigenschaften**.
5. Wählen Sie in dem sich öffnenden Fenster mit den Eigenschaften des Verteilungspunktes im Abschnitt **Allgemein** im linken Bereich von **Abschnitte** die Option **Diesen Verteilungspunkt als Push-Server verwenden** aus.
6. Geben Sie die Portnummer des Push-Servers an. Das ist der Port am Verteilungspunkt, den Client-Geräte für die Verbindung verwenden.

   Standardmäßig ist die Portnummer 13295 festgelegt.
7. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Verteilungspunkts zu schließen.
8. Öffnen Sie das Fenster mit den Richtlinieneinstellungen des Administrationsagenten.
9. Wechseln Sie im Abschnitt **Konnektivität** zum Unterabschnitt **Netzwerk**.

10. Wählen Sie im Unterabschnitt **Netzwerk** die Option **Verteilungspunkt verwenden, um eine Verbindung mit dem Administrationsserver zu erzwingen**.

11. Klicken Sie auf **OK**, um das Fenster zu verlassen.

Der Verteilungspunkt beginnt seine Arbeit als Push-Server. Es kann jetzt Push-Nachrichten an Client-Geräte senden.

Wenn Sie Geräte verwalten, auf denen KasperskyOS installiert ist, oder wenn Sie dies planen, müssen Sie einen Verteilungspunkt als Push-Server verwenden. Sie können einen Verteilungspunkt auch als Push-Server verwenden, wenn Sie Push-Nachrichten an Client-Geräte senden möchten.

Weitere Routinearbeiten

Dieser Abschnitt enthält Empfehlungen für die tägliche Arbeit mit Kaspersky Security Center.

Administrationsserver verwalten

Der Abschnitt enthält Informationen über die Arbeit mit den Administrationsservern und deren Einstellungen.

Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen

Sie können einen Administrationsserver als sekundären Administrationsserver hinzufügen und so eine Hierarchie vom Typ "primärer/sekundärer" festlegen. Das Hinzufügen eines sekundären Administrationsservers ist unabhängig davon möglich, ob der Administrationsserver, den Sie für die Verbindung über die Verwaltungskonsole sekundär machen wollen, verfügbar ist.

Bei der Zusammenfassung der Administrationsserver in der Hierarchie ist es erforderlich, dass der Port 13291 beider Server verfügbar ist. Der Port 13291 wird für die Annahme von Verbindungen von der Verwaltungskonsole zum Administrationsserver benötigt.

Verbindung des Administrationsservers als sekundärer Administrationsserver zum primären Administrationsserver

Sie können einen Administrationsserver als sekundären Server mit Verbindung zum primären Administrationsserver über den Port 13000 hinzufügen. Sie benötigen ein Gerät mit installierter Verwaltungskonsole, von dem aus die TCP-Ports 13291 beider Administrationsserver – des zukünftigen primären Administrationsservers und des zukünftigen sekundären Administrationsservers – verfügbar sind.

Um einen Administrationsserver, der für die Verbindung über die Verwaltungskonsole verfügbar ist, als sekundären Server hinzuzufügen:

1. Stellen Sie sicher, dass der Port 13000 des zukünftigen primären Administrationsservers für die Annahme von Verbindungen von sekundären Administrationsservern verfügbar ist.

2. Stellen Sie mithilfe der Verwaltungskonsole eine Verbindung zum zukünftigen primären Administrationsserver her.

3. Wählen Sie die Administrationsgruppe aus, zu der Sie den sekundären Administrationsserver hinzufügen möchten.

4. Im Arbeitsbereich des Knotens **Administrationsserver** der gewählten Gruppe klicken Sie dann auf den Link **Sekundären Administrationsserver hinzufügen**.

   Der Assistent für das Hinzufügen eines sekundären Administrationsservers wird gestartet.

5. Geben Sie im ersten Schritt des Assistenten (Adresse des Administrationsservers eingeben, der zur Gruppe hinzugefügt wird) den Netzwerknamen des zukünftigen sekundären Administrationsservers ein.

6. Folgen Sie den Anweisungen des Assistenten.

Die "primär/sekundär"-Hierarchie wird gebildet. Der primäre Administrationsserver übernimmt die Verbindung vom sekundären Administrationsserver.

Wenn Sie kein Gerät mit einer installierten Verwaltungskonsole haben, von dem aus die TCP-Ports 13291 beider Administrationsserver erreichbar sind, (wenn sich z. B. der zukünftige sekundäre Administrationsserver in einem Remote-Büro befindet und der Systemadministrator des Remote-Büros den Port 13291 aus Sicherheitsgründen nicht über das Internet verfügbar macht), können Sie den sekundären Server dennoch hinzufügen.

Um einen Administrationsserver, der nicht für die Verbindung über die Verwaltungskonsole verfügbar ist, als sekundären Server hinzuzufügen:

1. Stellen Sie sicher, dass der Port 13000 des zukünftigen primären Administrationsservers für die Verbindung von den sekundären Administrationsservern verfügbar ist.

2. Speichern Sie die Zertifikatsdatei des zukünftigen primären Administrationsservers auf einem externen Datenträger (z. B. einem USB-Stick) oder senden Sie diese an den Systemadministrator des Remote-Büros, in dem sich der Administrationsserver befindet.

   Die Datei mit dem Zertifikat des Administrationsservers befindet sich auf dem Administrationsserver unter der Adresse %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Speichern Sie die Zertifikatsdatei des zukünftigen sekundären Administrationsservers auf einem externen Datenträger (z. B. auf einem Flash-Drive). Wenn sich der zukünftige sekundäre Administrationsserver in einem Remote-Büro befindet, bitten Sie den Systemadministrator des Remote-Büros, Ihnen das Zertifikat zuzusenden.

   Die Datei mit dem Zertifikat des Administrationsservers befindet sich auf dem Administrationsserver unter der Adresse %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Stellen Sie mithilfe der Verwaltungskonsole eine Verbindung zum zukünftigen primären Administrationsserver her.

5. Wählen Sie die Administrationsgruppe aus, zu der Sie den sekundären Administrationsserver hinzufügen möchten.

6. Im Arbeitsbereich des Knotens **Administrationsserver** klicken Sie dann auf den Link **Sekundären Administrationsserver hinzufügen**.

   Der Assistent für das Hinzufügen eines sekundären Administrationsservers wird gestartet.

7. Lassen Sie im ersten Schritt des Assistenten (Eingabe der Adresse) das Feld **Adresse des sekundären Administrationsservers (optional)** leer.

8. Klicken Sie im Fenster **Zertifikatdatei des sekundären Administrationsservers** auf **Durchsuchen** und wählen Sie die zuvor gespeicherte Zertifikatsdatei des sekundären Administrationsservers aus.

9. Stellen Sie nach Fertigstellen des Assistenten mithilfe einer anderen Instanz der Verwaltungskonsole eine Verbindung zum zukünftigen sekundären Administrationsserver her. Wenn dieser Server sich in einem Remote-Büro befindet, bitten Sie den Systemadministrator des Remote-Büros, eine Verbindung zum zukünftigen sekundären Administrationsserver herzustellen und darauf die nächsten Schritte auszuführen.

10. Wählen Sie im Kontextmenü des Knotens **Administrationsserver** die Option **Eigenschaften** aus.

11. Wechseln Sie in den Eigenschaften des Administrationsservers zum Abschnitt **Erweitert** und dann weiter zum Unterabschnitt **Hierarchie der Administrationsserver**.

12. Aktivieren Sie das Kontrollkästchen **Dieser Administrationsserver ist in der Server-Hierarchie sekundär**.

    Die Eingabefelder werden für die Eingabe und die Bearbeitung verfügbar.

13. Geben Sie im Feld **Adresse des primären Administrationsservers** den Netzwerknamen des zukünftigen primären Administrationsservers an.

14. Wählen Sie die zuvor gespeicherte Zertifikatsdatei des zukünftigen primären Administrationsservers aus, indem Sie auf die Schaltfläche **Durchsuchen** klicken.

15. Klicken Sie auf die Schaltfläche **OK**.

Die "primär/sekundär"-Hierarchie wird gebildet. Sie können über die Verwaltungskonsole eine Verbindung mit dem sekundären Administrationsserver herstellen. Der primäre Administrationsserver übernimmt die Verbindung vom sekundären Administrationsserver.

Verbindung des primären Administrationsservers mit dem sekundären Administrationsserver

Sie können einen neuen Administrationsserver als sekundär hinzufügen, so dass der primäre Administrationsserver über den Port 13000 mit dem sekundären Administrationsserver verbunden wird. Das ist beispielsweise zweckmäßig, wenn Sie den sekundären Administrationsserver in der demilitarisierten Zone platzieren.

Sie benötigen ein Gerät mit installierter Verwaltungskonsole, von dem aus die TCP-Ports 13291 beider Administrationsserver – des zukünftigen primären Administrationsservers und des zukünftigen sekundären Administrationsservers – verfügbar sind.

Um einen neuen Administrationsserver als sekundär hinzuzufügen und den primären Administrationsserver über den Port 13000 mit ihm zu verbinden:

1. Stellen Sie sicher, dass der Port 13000 des zukünftigen sekundären Administrationsservers für die Annahme von Verbindungen vom primären Administrationsserver verfügbar ist.

2. Stellen Sie mithilfe der Verwaltungskonsole eine Verbindung zum zukünftigen primären Administrationsserver her.

3. Wählen Sie die Administrationsgruppe aus, zu der Sie den sekundären Administrationsserver hinzufügen möchten.

4. Im Arbeitsbereich des Knotens **Administrationsserver** der relevanten Administrationsgruppe klicken Sie dann auf den Link **Sekundären Administrationsserver hinzufügen**.

   Der Assistent für das Hinzufügen eines sekundären Administrationsservers wird gestartet.

5. Geben Sie im ersten Schritt des Assistenten (Adresse des Administrationsservers eingeben, der zur Gruppe hinzugefügt wird) den Netzwerknamen des zukünftigen sekundären Administrationsservers ein und aktivieren Sie das Kontrollkästchen **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**.

6. Wenn Sie die Verbindung mit dem zukünftigen sekundären Administrationsserver über einen Proxyserver herstellen, aktivieren Sie im ersten Schritt des Assistenten das Kontrollkästchen **Proxyserver benutzen** und geben Sie die Verbindungseinstellungen ein.

7. Folgen Sie den Anweisungen des Assistenten.

Die Hierarchie der Administrationsserver wird festgelegt. Der sekundäre Administrationsserver übernimmt die Verbindung vom primären Administrationsserver.

Verbindung mit dem Administrationsserver herstellen und zwischen Administrationsservern wechseln

Beim Starten versucht Kaspersky Security Center, eine Verbindung zum Administrationsserver herzustellen. Wenn im Netzwerk mehrere Administrationsserver vorhanden sind, wird der Server abgefragt, mit dem eine Verbindung während der letzten Sitzung von Kaspersky Security Center hergestellt wurde.

> Wird das Programm zum ersten Mal nach der Installation gestartet, so wird eine Verbindung mit dem Administrationsserver hergestellt, der bei der Installation von Kaspersky Security Center angegeben wurde.

Nachdem die Verbindung mit dem Administrationsserver hergestellt wurde, wird die Ordnerstruktur dieses Servers in der Konsolenstruktur angezeigt.

Wurden zur Konsolenstruktur mehrere Administrationsserver hinzugefügt, können Sie zwischen ihnen wechseln.

Für die Verwendung jedes Administrationsservers wird eine die Verwaltungskonsole benötigt. Stellen Sie vor der ersten Verbindung mit einem neuen Administrationsserver sicher, dass auf diesem der Port 13291, über den die Verbindungen von der Verwaltungskonsole eingehen, sowie alle anderen Ports für die Verbindung des Administrationsservers mit anderen Komponenten von Kaspersky Security Center geöffnet sind.

Um zu einem anderen Administrationsserver zu wechseln, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

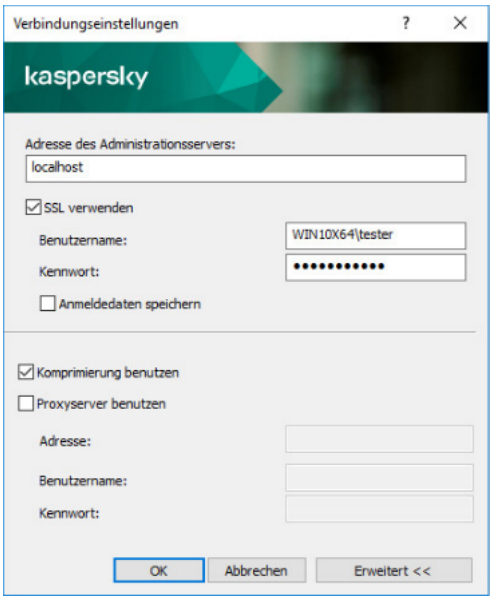
2. Wählen Sie im Kontextmenü des Knotens **Mit dem Administrationsserver verbinden** aus.

3. Geben Sie im folgenden Fenster **Verbindungseinstellungen** im Feld **Adresse des Administrationsservers** den Namen des Administrationsservers an, mit dem eine Verbindung hergestellt werden soll. Als Name des Administrationsservers können Sie die IP-Adresse oder den Gerätenamen im Windows-Netzwerk angeben. Mit der Schaltfläche **Erweitert** im unteren Bereich des Fensters können Sie die Verbindungseinstellungen mit dem Administrationsserver anpassen.

Zur Verbindung mit dem Administrationsserver über einen Port, der sich vom standardmäßigen Port unterscheidet, geben Sie im Feld **Adresse des Administrationsservers** einen Wert im Format <Name des Administrationsservers>:<Port> an.

Um eine Verbindung mit einem virtuellen Administrationsserver herzustellen, geben Sie im Feld **Adresse des Administrationsservers** einen Wert im Format "<Adresse des Administrationsservers>/<Name des virtuellen Servers>" ein.

Die Benutzer, die über keine Berechtigung zum **Lesen** verfügen, können nicht auf den Administrationsserver zugreifen.



Herstellen einer Verbindung mit dem Administrationsserver

4. Klicken Sie auf **OK**, um das Umschalten zwischen den Servern abzuschließen.

   Nach der Verbindung mit dem Administrationsserver wird die Ordnerstruktur des entsprechenden Knotens in der Konsolenstruktur aktualisiert.

Zugriffsberechtigungen für den Administrationsserver und dessen Objekte

Bei der Installation von Kaspersky Security Center werden die Gruppen **KLAdmins** und **KLOperators** automatisch erstellt. Diesen Gruppen werden die Rechte für die Verbindung mit dem Administrationsserver und die Bearbeitung der Serverobjekte gewährt.

Abhängig davon, unter welchem Benutzerkonto Kaspersky Security Center installiert wird, werden die Gruppen **KLAdmins** und **KLOperators** auf folgende Weise erstellt:

- Wenn die Installation unter dem Benutzerkonto eines Benutzers ausgeführt wird, der zur Domäne gehört, werden die Gruppen in der Domäne, zu welcher der Administrationsserver gehört, sowie auf dem Administrationsserver erstellt.

- Wenn die Installation unter dem System-Benutzerkonto ausgeführt wird, werden die Gruppen nur auf dem Administrationsserver erstellt.

Die Gruppen **KLAdmins** und **KLOperators** lassen sich mit den Standard-Administrationsfunktionen des Betriebssystems anzeigen. Mit denselben Funktionen können erforderliche Änderungen an den Benutzerrechten der Gruppen **KLAdmins** und **KLOperators** vorgenommen werden.

Die Gruppe **KLAdmins** verfügt über alle Berechtigungen, die Gruppe **KLOperators** nur über die Berechtigungen Lesen und Ausführen. Die Rechte der Gruppe **KLAdmins** können nicht geändert werden.

Die Benutzer, die zur Gruppe **KLAdmins** gehören, werden als *Administratoren von Kaspersky Security Center* bezeichnet, die Benutzer aus der Gruppe **KLOperators** werden als *Kaspersky Security Center Operatoren* bezeichnet.

Neben den Benutzern, die zur Gruppe **KLAdmins** gehören, werden die Administratorrechte von Kaspersky Security Center lokalen Administratoren von Geräten vergeben, auf denen der Administrationsserver installiert ist.

Sie können lokale Administratoren aus der Liste der Benutzer ausschließen, die über die Rechte des Administrators von Kaspersky Security Center verfügen.

Alle Vorgänge, die von den Administratoren von Kaspersky Security Center gestartet werden, werden mit den Rechten des Administrationsserver-Benutzerkontos ausgeführt.

Für jeden Administrationsserver im Netzwerk können Sie die einzelne Gruppe **KLAdmins** erstellen, die über die Rechte für die Arbeit nur mit diesem Server verfügt.

Wenn Geräte einer Domäne zu Administrationsgruppen verschiedener Administrationsserver gehören, ist der Administrator der Domäne im Rahmen aller dieser Administrationsgruppen gleichzeitig ein Administrator von Kaspersky Security Center. Die Gruppe **KLAdmins** ist dabei für diese Administrationsgruppen einheitlich und wird bei der Installation des ersten Administrationsservers angelegt. Vorgänge, die vom Administrator von Kaspersky Security Center gestartet werden, werden mit den Rechten des Benutzerkontos des Administrationsservers ausgeführt, für den sie gestartet wurden.

Nach der Programminstallation kann der Administrator von Kaspersky Security Center folgende Aktionen ausführen:

- Rechte ändern, welche an die Gruppen **KLOperators** vergeben werden
- Gewähren von Zugriffsrechten auf die Funktionen von Kaspersky Security Center für andere Sicherheitsgruppen und einzelne Benutzer, die auf dem Administrator-Arbeitsplatz registriert wurden
- Zugriffsrechte für Benutzer in jeder Administrationsgruppe bestimmen

Der Administrator von Kaspersky Security Center kann Zugriffsrechte auf jede Administrationsgruppe oder auf andere Objekte des Administrationsservers separat im Abschnitt **Sicherheit** des Eigenschaftenfensters eines gewählten Objekts bestimmen.

Sie können Benutzeraktionen mit den Datenträgern über Ereignisse des Administrationsservers verfolgen. Einträge zu Ereignissen werden im Knoten **Administrationsserver** auf der Registerkarte **Ereignisse** angezeigt. Diese Ereignisse haben die Ereigniskategorie **Informative Ereignisse**, die Ereignistypen beginnen mit dem Wort **Audit**.

Bedingungen für das Herstellen einer Internetverbindung mit dem Administrationsserver

Wenn sich der Administrationsserver an einem Remotestandort (außerhalb des Firmennetzwerks) befindet, werden die Client-Geräte via Internet mit diesem verbunden.

Zum Herstellen einer Internetverbindung zwischen Geräten und dem Administrationsserver müssen folgende Bedingungen erfüllt sein:

- Der Remote-Administrationsserver benötigt eine externe IP-Adresse, wobei der Eingangsport 13000 (für Verbindungen von Administrationsagenten) geöffnet sein muss. Es wird empfohlen, zusätzlich den UDP-Port 13000 (für die Annahme von Benachrichtigungen über die Deaktivierung von Geräten) zu öffnen.

- Auf den Geräten müssen Administrationsagenten installiert sein.

- Bei der Installation des Administrationsagenten auf den Geräten muss die IP-Adresse des Remote-Administrationsservers angegeben werden. Wenn für die Installation ein Installationspaket verwendet wird, muss die externe IP-Adresse manuell in den Eigenschaften des Installationspaketes im Abschnitt **Einstellungen** eingegeben werden.

- Um Programme und Aufgaben eines Geräts mit dem Administrationsserver verwalten zu können, aktivieren Sie im Eigenschaftenfenster des Geräts im Abschnitt **Allgemein** das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**. Nachdem Sie das Kontrollkästchen aktiviert haben, warten Sie auf die Synchronisierung des Administrationsservers mit dem Remote-Gerät. Eine ununterbrochene Verbindung mit dem Administrationsserver wird für maximal 300 Client-Geräte zugleich unterstützt.

Um die Ausführung der Aufgaben zu beschleunigen, die vom Remote-Administrationsserver eingehen, können Sie auf dem Gerät den Port 15000 öffnen. In diesem Fall sendet der Administrationsserver zum Starten der Aufgabe über den Port 15000 ein spezielles Paket an den Administrationsagenten, ohne auf den Abschluss der Synchronisierung mit dem Gerät zu warten.

Geschützte Verbindung mit dem Administrationsserver einrichten

Der Datenaustausch zwischen Client-Geräten und dem Administrationsserver sowie die Verbindung der Verwaltungskonsole mit dem Administrationsserver können per TLS-Protokoll (Transport Layer Security) erfolgen. Das TLS-Protokoll identifiziert die miteinander agierenden Seiten, führt eine Verschlüsselung der Datenübertragung durch und schützt sie vor Veränderungen bei der Übertragung. Das TLS-Protokoll basiert auf der Authentifizierung der miteinander agierenden Stellen und die Datenverschlüsselung mit offenen Schlüsseln.

Authentifizierung des Administrationsservers beim Verbinden des Geräts

Beim ersten Verbindungsaufbau zwischen einem Client-Gerät und dem Administrationsserver, empfängt der Administrationsagent auf dem Gerät eine Kopie des Zertifikats des Administrationsservers und speichert sie lokal.

> Bei einer lokalen Installation des Administrationsagenten auf einem Gerät können Sie das Zertifikat des Administrationsservers manuell wählen.

Anhand der empfangenen Zertifikatskopie werden die Berechtigungen und Rechte des Administrationsservers bei den nachfolgenden Verbindungen überprüft.

Zusätzlich fragt der Administrationsagent bei jeder Verbindung des Geräts mit dem Administrationsserver das Zertifikat des Administrationsservers ab und vergleicht es mit der lokalen Kopie. Wenn sie nicht übereinstimmen, kann der Administrationsserver nicht auf das Gerät zugreifen.

Authentifizierung des Administrationsservers beim Verbindungsaufbau mit der Verwaltungskonsole

Beim ersten Verbindungsaufbau zum Administrationsserver nach der Installation fragt die Verwaltungskonsole das Zertifikat des Administrationsservers ab und speichert seine Kopie lokal auf dem Administrator-Arbeitsplatz. Anhand der empfangenen Zertifikatskopie wird der Administrationsserver bei nachfolgenden Verbindungen mit der Verwaltungskonsole identifiziert.

Wenn das Zertifikat des Administrationsservers nicht mit der auf dem Administrator-Arbeitsplatz gespeicherten Zertifikatskopie übereinstimmt, werden von der Verwaltungskonsole eine Bestätigung der Verbindung zum Administrationsserver mit dem angegebenen Namen und der Download eines neuen Zertifikats angefordert. Nach der Verbindung speichert die Verwaltungskonsole die Kopie des neuen Zertifikats des Administrationsservers, die zur künftigen Identifizierung des Servers dient.

Eine Allow-Liste von IP-Adressen für die Verbindung mit dem Administrationsserver konfigurieren

Standardmäßig können sich Benutzer auf jedem Gerät, auf dem sie die Kaspersky Security Center Web Console (im Folgenden als Web Console bezeichnet) öffnen können, oder auf dem die MMC-basierte Verwaltungskonsole installiert ist, an Kaspersky Security Center anmelden. Sie können den Administrationsserver jedoch auch so konfigurieren, dass Benutzer nur von Geräten mit zugelassenen IP-Adressen eine Verbindung zu ihm herstellen dürfen. Selbst wenn ein Eindringling an die Anmeldedaten eines Benutzerkontos von Kaspersky Security Center gelangt, kann er sich in diesem Fall nicht bei Kaspersky Security Center anmelden, da die IP-Adresse des Geräts des Eindringlings nicht auf der Allow-Liste steht.

Die IP-Adresse wird überprüft, wenn sich ein Benutzer an Kaspersky Security Center anmeldet oder eine Anwendung ausführt, die mit dem Administrationsserver über Kaspersky Security Center OpenAPI interagiert. In so einem Moment versucht das Gerät des Benutzers, eine Verbindung mit dem Administrationsserver herzustellen. Befindet sich die IP-Adresse des Geräts nicht auf der Allow-Liste, tritt ein Authentifizierungsfehler auf und das Ereignis KLAUD_EV_SERVERCONNECT benachrichtigt Sie darüber, dass eine Verbindung mit dem Administrationsserver abgelehnt wurde.

Anforderungen an eine Allow-Liste mit IP-Adressen

IP-Adressen werden nur überprüft, wenn die folgenden Programme versuchen, sich mit dem Administrationsserver zu verbinden:

- Server der Web Console

  Wenn Sie sich auf einem Gerät an der Web Console anmelden und der Server der Web Console auf einem anderen Gerät installiert ist, können Sie auf dem Gerät mit installierter Web Console eine Firewall konfigurieren, indem Sie die Standardmittel des Betriebssystems verwenden. Wenn anschließend jemand versucht, sich an der Web Console anzumelden, hilft eine Firewall dabei, Eingriffe durch Eindringlinge abzuwehren.

- Verwaltungskonsole
- Programme, die mittels klakaut-Automatisierungsobjekten mit dem Administrationsserver interagieren
- Anwendungen, die mittels OpenAPI mit dem Administrationsserver interagieren, z. B. Kaspersky Anti Targeted Attack Platform oder Kaspersky Security for Virtualization

Geben Sie daher Adressen der Geräte an, auf denen die oben aufgeführten Anwendungen installiert sind.

Sie können sowohl IPv4- als auch IPv6-Adressen angeben. Sie können keine IP-Adressbereiche angeben.

So erstellen Sie eine Allow-Liste mit IP-Adressen

Wenn Sie zuvor noch keine Allow-Liste erstellt haben, folgen Sie den nachstehenden Anweisungen.

So erstellen Sie die Allow-Liste mit IP-Adressen zur Anmeldung an Kaspersky Security Center:

1. Führen Sie auf dem Gerät des Administrationsservers die Eingabeaufforderung unter einem Konto mit Administratorrechten aus.

2. Ändern Sie Ihr aktuelles Verzeichnis in den Installationsordner von Kaspersky Security Center (standardmäßig <Laufwerk>:\Programme (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Geben Sie den folgenden Befehl mit Administratorrechten ein:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP-Adressen>" -t s`

   Geben Sie IP-Adressen an, die den oben aufgeführten Anforderungen entsprechen. Mehrere IP-Adressen müssen durch ein Semikolon getrennt werden.

   Beispiel, um nur einem Gerät die Verbindung mit dem Administrationsserver zu erlauben:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Beispiel, um mehreren Geräten die Verbindung mit dem Administrationsserver zu erlauben:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`

4. Starten Sie den Dienst des Administrationsservers neu.

Dem Kaspersky-Ereignisprotokoll des Administrationsservers können Sie entnehmen, ob Sie die Allow-Liste mit IP-Adressen erfolgreich konfiguriert haben.

So ändern Sie eine Allow-Liste mit IP-Adressen

Sie können eine Allow-Liste auf gleiche Weise ändern, wie Sie es bei der erstmaligen Erstellung getan haben. Führen Sie daher denselben Befehl aus und geben Sie eine neue Allow-Liste an:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP-Adressen>" -t s
```

Wenn Sie einige IP-Adressen aus der Allow-Liste löschen möchten, erstellen Sie diese neu. Ihre Allow-Liste enthält beispielsweise die folgenden IP-Adressen: 192.0.2.0; 198.51.100.0 und 203.0.113.0. Sie möchten die IP-Adresse 198.51.100.0 aus der Liste löschen. Geben Sie dafür den folgenden Befehl in die Eingabeaufforderung ein:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Stellen Sie sicher, den Dienst des Administrationsservers neu zu starten.

Zurücksetzen einer konfigurierten Allow-Liste mit IP-Adressen

So setzen Sie eine bereits konfigurierte Allow-Liste mit IP-Adressen zurück:

1. Geben Sie den folgenden Befehl mit Administratorrechten in die Eingabeaufforderung ein:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Starten Sie den Dienst des Administrationsservers neu.

Anschließend werden IP-Adressen nicht mehr überprüft.

Klscflag-Tool zum Schließen von Port 13291 verwenden

Auf dem Administrationsserver wird Port 13291 zum Empfangen der Verbindungen von Verwaltungskonsolen verwendet. Dieser Port ist standardmäßig geöffnet. Wenn Sie die MMC-basierte Verwaltungskonsole oder das klakaut-Tool nicht verwenden möchten, können Sie diesen Port mit dem klscflag-Tool schließen. Dieses Tool ändert den Wert des Parameters KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

So schließen Sie Port 13291:

1. Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

2. Führen Sie den folgenden Befehl in der Befehlszeile aus:
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -
   svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```

3. Starten Sie den Dienst des Kaspersky Security Center Administrationsservers neu.

   Der Port 13291 ist geschlossen.

So überprüfen Sie, ob Port 13291 erfolgreich geschlossen wurde:

Führen Sie den folgenden Befehl in der Befehlszeile aus:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -
ss "|ss_type = \"SS_SETTINGS\";"
```

Dieser Befehl gibt das folgende Ergebnis zurück:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

Der Wert `false` bedeutet, dass der Port geschlossen ist. Ansonsten wird der Wert `true` angezeigt.

Verbindung mit dem Administrationsserver trennen

Um die Verbindung mit dem Administrationsserver zu trennen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten aus, der dem Administrationsserver entspricht, dessen Verbindung getrennt werden muss.
2. Wählen Sie im Kontextmenü des Knotens **Vom Administrationsserver trennen** aus.

Administrationsserver zur Konsolenstruktur hinzufügen

Um der Konsolenstruktur einen Administrationsserver hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von Kaspersky Security Center in der Konsolenstruktur den Knoten **Kaspersky Security Center**.
2. Wählen Sie im Kontextmenü des Knotens den Punkt **Neu → Administrationsserver** aus.

In der Konsolenstruktur wird dadurch ein Knoten mit dem Namen **Administrationsserver –<Gerätename> (Nicht verbunden)** erstellt, von dem aus Sie eine Verbindung zu einem beliebigen der im Netzwerk installierten Administrationsserver herstellen können.

Administrationsserver aus der Konsolenstruktur entfernen

Um einen Administrationsserver aus der Konsolenstruktur zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten aus, der dem zu entfernenden Administrationsserver entspricht.
2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **Entfernen** aus.

Hinzufügen eines virtuellen Administrationsservers zur Konsolenstruktur hinzufügen

Um der Konsolenstruktur einen virtuellen Administrationsserver hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des benötigten Administrationsservers aus, für den ein virtueller Administrationsserver erstellt werden soll.
2. Wählen Sie im Knoten des Administrationsservers den Ordner **Administrationsserver** aus.
3. Klicken Sie im Arbeitsbereich des Ordners **Administrationsserver** auf den Link **Virtuellen Administrationsserver hinzufügen**.

   Daraufhin wird der Assistent für das Erstellen eines virtuellen Administrationsservers gestartet.

4. Geben Sie im Fenster **Name des virtuellen Administrationsservers** den Namen des virtuellen Administrationsservers an, den Sie erstellen möchten.

   Der Name der virtuellen Administrationsservers darf nicht mehr als 255 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|).

5. Geben Sie im Fenster **Geben Sie die Adresse an, über welche die Geräte mit dem virtuellen Administrationsserver verbunden werden sollen** die Adresse für die Verbindung des Gerätes an

   Die Adresse der Verbindung des virtuellen Administrationsservers ist eine Netzwerkadresse, über die Geräte an den Server angeschlossen werden. Die Adresse der Verbindung besteht aus zwei Teilen: der Netzwerkadresse des physischen Administrationsservers und dem Namen des virtuellen Administrationsservers (mit Schrägstrich getrennt). Der Name des virtuellen Administrationsservers wird automatisch eingetragen. Die angegebene Adresse wird auf diesem virtuellen Administrationsserver als Standardadresse in den Installationspaketen des Administrationsagenten verwendet.

6. Bestimmen Sie im Fenster **Konto für den Administrator des virtuellen Administrationsservers erstellen** einen Benutzer aus der Liste zum Administrator des virtuellen Servers oder fügen Sie ein neues Benutzerkonto für den Administrator über die Schaltfläche **Erstellen** hinzu.

   Sie können mehrere Benutzerkonten angeben.

Daraufhin wird in der Konsolenstruktur der Knoten **Administrationsserver <Name des virtuellen Administrationsservers>** erstellt.

Benutzerkonto des Administrationsserver-Dienstes wechseln. Tool klsrvswch

Wenn es erforderlich ist, das Benutzerkonto für Dienst des Administrationsservers zu wechseln, das bei der Installation von Kaspersky Security Center vorgegeben wurde, können Sie das Tool "klsrvswch" verwenden, das zum Wechseln des Benutzerkontos des Administrationsservers dient.

Bei der Installation von Kaspersky Security Center wird das Tool automatisch in den Installationsordner der Anwendung kopiert.

Die Tools kann beliebig oft gestartet werden.

Sie müssen das Tool "klsrvswch" auf dem Administrationsserver unter demselben Benutzerkonto mit Administratorrechten starten, das für die Installation des Administrationsservers verwendet wurde.

Das Tool "klsrvswch" erlaubt Ihnen, den Typ des Benutzerkontos zu ändern. Wenn Sie beispielsweise ein lokales Benutzerkonto verwenden, können Sie stattdessen zum Domänenbenutzerkonto oder zum verwalteten Benutzerkonto für den Dienst wechseln (und umgekehrt). Mit dem Tool "klsrvswch" können Sie den Kontotyp nicht in einen gruppenverwaltetes Dienstkonto (Group Managed Service Account – gMSA) ändern.

Windows Vista und spätere Windows-Versionen erlauben keine Verwendung des Kontos "LocalSystem" für den Administrationsserver. In diesen Windows-Versionen, ist die **Konto-Option "LocalSystem"** inaktiv.

Um das Benutzerkonto für Dienst des Administrationsservers auf ein Domänenbenutzerkonto zu ändern, gehen Sie wie folgt vor:

1. Starten Sie das Tool "klsrvswch" aus dem Installationsordner von Kaspersky Security Center. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

   Daraufhin wird der Assistent zum Wechseln des Administrationsserver-Benutzerkontos gestartet. Folgen Sie den Anweisungen des Assistenten.

2. Wählen Sie im Fenster **Benutzerkonto für Dienst des Administrationsservers** die **Konto-Option "LocalSystem"**.

Nach Abschluss des Assistenten wird das Benutzerkonto des Administrationsservers geändert. Der Dienst des Administrationsservers wird unter dem Benutzerkonto und mit den Anmeldedaten des *Kontos "LocalSystem"* gestartet.

Damit Kaspersky Security Center fehlerfrei funktioniert, muss das Benutzerkonto für den Start des Administrationsservers über die Administratorrechte für das Speichern der Administrationsserver-Datenbank verfügen.

Um ein Benutzerkonto für Dienst des Administrationsservers auf ein Benutzerkonto oder ein verwaltetes Benutzerkonto für den Dienst zu ändern, gehen Sie wie folgt vor:

1. Starten Sie das Tool "klsrvswch" aus dem Installationsordner von Kaspersky Security Center. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

   Daraufhin wird der Assistent zum Wechseln des Administrationsserver-Benutzerkontos gestartet. Folgen Sie den Anweisungen des Assistenten.

2. Wählen Sie im Fenster **Benutzerkonto für Dienst des Administrationsservers** die Option **Benutzerdefiniertes Konto**.

3. Klicken Sie auf die Schaltfläche **Suchen**.

   Das Fenster **Wählen Sie einen Benutzer aus** wird geöffnet.

4. Klicken Sie im Fenster **Wählen Sie einen Benutzer aus** auf die Schaltfläche **Objekttypen**.

5. Wählen Sie in der Liste der Objekttypen **Benutzer** (wenn Sie ein Benutzerkonto möchten) oder **Benutzerkonten für den Dienst** (wenn Sie ein verwaltetes Benutzerkonto für den Dienst möchten) aus und klicken Sie auf **OK**.

6. Geben Sie im Feld für den Objektnamen den Namen des Benutzerkontos oder einen Teil des Namens ein und klicken Sie auf **Namen überprüfen**.

7. Wählern Sie in der Liste der übereinstimmenden Namen den gewünschten Namen aus und klicken Sie auf **OK**.

8. Wenn Sie **Benutzerkonten für den Dienst** ausgewählt haben, lassen Sie im Fenster **Kennwort des Benutzerkontos** die Felder **Kennwort** und **Kennwort bestätigen** leer. Wenn Sie **Benutzer** ausgewählt haben, geben Sie ein neues Kennwort für den Benutzer ein und bestätigen Sie es.

Das Benutzerkonto für Dienst des Administrationsservers wird auf das ausgewählte Benutzerkonto geändert.

Bei Verwendung von Microsoft SQL Server in einem Modus, der als Vorbedingung Benutzerkonto-Authentifizierung mithilfe von Windows-Tools enthält, muss Zugriff auf die Datenbank gewährt werden. Das Benutzerkonto muss dem Besitzer der Datenbank von Kaspersky Security Center zugewiesen sein. Standardmäßig ist das Schema dbo zu verwenden.

DBMS-Anmeldedaten ändern

Möglicherweise müssen Sie die DBMS-Anmeldedaten ändern, etwa um aus Sicherheitsgründen eine Rotation der Anmeldedaten zu realisieren.

Um die DBMS-Anmeldedaten in einer Windows-Umgebung mithilfe von klsrvswch.exe zu ändern:

1. Starten Sie das Tool klsrvswch, das sich im Installationsordner von Kaspersky Security Center befindet. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

   Sie müssen das Tool "klsrvswch" auf dem Administrationsserver unter demselben Benutzerkonto mit Administratorrechten starten, das für die Installation des Administrationsservers verwendet wurde.

2. Klicken Sie im Assistenten auf **Weiter**, bis Sie den Schritt **Anmeldedaten für DBMS-Zugriff ändern** erreichen.

3. Führen Sie beim Schritt **Anmeldedaten für DBMS-Zugriff ändern** des Assistenten die folgenden Aktionen aus:

   Wenn die Windows-Anmeldung verwendet wird, wird im Assistenten der Schritt **Anmeldedaten für DBMS-Zugriff ändern** übersprungen.

   - Wählen Sie die Option **Neue Anmeldedaten anwenden** aus.
   - Geben Sie im Feld **Benutzerkonto** einen neuen Namen für das Benutzerkonto an.
   - Geben Sie im Feld **Kennwort** ein neues Kennwort für das Benutzerkonto an.
   - Wiederholen Sie das neue Kennwort im Feld **Kennwort bestätigen**.

   Sie sollten die Anmeldedaten eines Benutzerkontos angeben, das im DBMS vorhanden ist.

4. Klicken Sie auf **Weiter**.

Nach Abschluss des Assistenten werden die DBMS-Anmeldedaten geändert.

Das Tool "klsrvswch" kann nur verwendet werden, um das Kennwort des Benutzerkontos für die SQL-Authentifikation zu ändern. Das Ändern der zur Authentifikation verwendeten Methode wird nicht unterstützt. Wenn Sie die zur Authentifikation verwendete Methode möchten, installieren Sie den Administrationsserver erneut und geben Sie die gewünschten Einstellungen an.

Den freigegebenen Ordner des Administrationsservers ändern

Der freigegebene Ordner des Administrationsservers wird während der Installation des Administrationsservers angegeben. Sie können den Ort des freigegebenen Ordners nach der Installation in den Eigenschaften des Administrationsservers ändern.

So ändern Sie den freigegebenen Ordner:

1. Erstellen Sie einen freigegebenen Netzwerkordner und konfigurieren Sie Berechtigungen für die Freigabe und die Ordnerstruktur so, dass die Untergruppe **Jeder** volle Zugriffsberechtigungen dafür besitzt.
2. Öffnen Sie in der Konsolenstruktur von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie den Punkt **Eigenschaften** aus.
3. Wählen Sie im Bereich **Abschnitte** des Fensters "Eigenschaften des Administrationsservers" die Option **Erweitert** und anschließend **Freigegebener Ordner des Administrationsservers** aus.
4. Klicken Sie im Abschnitt **Freigegebener Ordner des Administrationsservers** auf **Ändern**.
5. Wählen Sie den Ordner aus, den Sie als freigegebenen Order verwenden möchten.
6. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Administrationsservers zu schließen.
7. Gewähren Sie der untergeordneten Gruppe **Jeder** für den Ordner, den Sie als freigegebenen Ordner ausgewählt haben, das Leserecht.

Probleme mit den Knoten des Administrationsservers lösen

Die Konsolenstruktur im linken Bereich der Verwaltungskonsole enthält die Knoten der Administrationsserver. Sie können beliebig viele Administrationsserver zur Konsolenstruktur hinzufügen.

Die Liste mit Administrationsserver-Knoten in der Konsolenstruktur wird mittels der Microsoft Management Console in der Schattenkopie einer .msc-Datei gespeichert. Die Schattenkopie dieser Datei befindet sich im Ordner %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ auf dem Gerät, auf dem die Verwaltungskonsole installiert ist. Für jeden Administrationsserver-Knoten enthält die Datei die folgenden Informationen:

- Adresse des Administrationsservers
- Portnummer
- Wird TLS verwendet?

  Dieser Wert ist abhängig vom Port, über den die Verwaltungskonsole mit dem Administrationsserver verbunden wird.

- Benutzername
- Zertifikat des Administrationsservers

Problemlösung

Wenn die Verwaltungskonsole mit dem Administrationsserver verbunden wird, wird das lokal gespeicherte Zertifikat mit dem Zertifikat des Administrationsservers verglichen. Stimmen die Zertifikate nicht überein, so generiert die Verwaltungskonsole einen Fehler. Eine Nichtübereinstimmung kann z. B. erfolgen, wenn Sie das Zertifikat des Administrationsservers ersetzen. In einem solchen Fall müssen Sie den Administrationsserver-Knoten in der Konsole erneut erstellen.

Um einen Administrationsserver-Knoten erneut zu erstellen, gehen Sie wie folgt vor:

1. Schließen Sie das Fenster der Kaspersky Security Center Verwaltungskonsole.
2. Löschen Sie die Datei für Kaspersky Security Center 15.1 in %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Starten Sie die Kaspersky Security Center Verwaltungskonsole.

   Sie werden aufgefordert, eine Verbindung zum Administrationsserver herzustellen und das vorhandene Zertifikat zu akzeptieren.
4. Führen Sie eine der folgenden Aktionen aus:
   - Akzeptieren Sie das vorhandene Zertifikat über die Schaltfläche **Ja**.
   - Um Ihr eigenes Zertifikat anzugeben, klicken Sie auf **Nein** und finden Sie dann die Zertifikatsdatei, die zur Authentifizierung des Administrationsservers verwendet werden soll.

Das Zertifikatsproblem ist nun gelöst. Sie können die Verwaltungskonsole zur Verbindung mit dem Administrationsserver nutzen.

Einstellungen des Administrationsservers anzeigen und ändern

Sie können die Einstellungen des Administrationsservers in seinem Eigenschaftenfenster anpassen.

Um das Eigenschaftenfenster des Administrationsservers zu öffnen,

klicken Sie mit der rechten Maustaste auf den Knoten des Administrationsservers und wählen Sie **Eigenschaften** aus.

Allgemeine Einstellungen des Administrationsservers konfigurieren

Sie können allgemeine Einstellungen des Administrationsservers in den Abschnitten **Allgemein**, **Verbindungseinstellungen des Administrationsservers**, **Ereignis-Datenverwaltung** und **Sicherheit** im Eigenschaftenfenster des Administrationsservers anpassen.

Der Abschnitt **Sicherheit** wird nicht im Eigenschaftenfenster des Administrationsservers angezeigt, wenn die Anzeige in der Benutzeroberfläche der Verwaltungskonsole deaktiviert ist.

*Um die Ansicht des Abschnitts **Sicherheit** in der Verwaltungskonsole zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den erforderlichen Administrationsserver aus.
2. Wählen Sie im Programmhauptfenster im Menü **Ansicht** den Punkt **Benutzeroberfläche anpassen**.
3. Aktivieren Sie in dem sich öffnenden Fenster **Benutzeroberfläche anpassen** das Kontrollkästchen **Abschnitte mit Sicherheitseinstellungen anzeigen** und klicken Sie auf **OK**.
4. Klicken Sie im Fenster mit den Programm-Meldungen auf die Schaltfläche **OK**.

Der Abschnitt **Sicherheit** wird im Eigenschaftenfenster des Administrationsservers angezeigt.

Schnittstelleneinstellungen der Verwaltungskonsole

Sie können die Schnittstelleneinstellungen der Verwaltungskonsole anpassen, um die Benutzeroberflächen-Steuerelemente anzuzeigen oder zu verbergen, die zu den folgenden Funktionen gehören:

- Schwachstellen- und Patch-Management
- Verschlüsselung und Datenschutz
- Einstellungen für "Endpoint Control"
- Verwaltung mobiler Geräte
- Sekundäre Administrationsserver
- Abschnitte für "Sicherheitseinstellungen"

Um die Schnittstelleneinstellungen der Verwaltungskonsole anzupassen:

1. Wählen Sie in der Konsolenstruktur den erforderlichen Administrationsserver aus.
2. Wählen Sie im Programmhauptfenster im Menü **Ansicht** den Punkt **Benutzeroberfläche anpassen**.
3. Aktivieren Sie im folgenden Fenster **Benutzeroberfläche anpassen** die Kontrollkästchen für die Funktionen, die angezeigt werden sollen, und klicken Sie auf **OK**.
4. Klicken Sie im Fenster mit den Programm-Meldungen auf die Schaltfläche **OK**.

Die ausgewählten Funktionen werden auf der Benutzeroberfläche der Verwaltungskonsole angezeigt.

Ereignisse auf dem Administrationsserver verarbeiten und speichern

Die Informationen zu Ereignissen, die während der Ausführung der Anwendung und der verwalteten Geräte auftreten, werden in der Administrationsserver-Datenbank gespeichert. Jedes Ereignis gehört einem bestimmten Typ und einer Signifikanz (*Kritisches Ereignis*, *Funktionsfehler*, *Warnung*, *Infomeldung*) an. Abhängig von den Umständen, unter denen das Ereignis aufgetreten ist, können Ereignissen eines Typs von der Anwendung verschiedene Signifikanzen zugeordnet werden.

Die Typen und Signifikanzen können Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignisse konfigurieren** anzeigen. Ferner können Sie im Abschnitt **Ereignisse konfigurieren** die Einstellungen für die Verarbeitung der einzelnen Ereignisse durch den Administrationsserver anpassen:

- Ereignisse auf dem Administrationsserver und in den Ereignisprotokollen des Betriebssystems auf dem Gerät und auf dem Administrationsserver erfassen
- Benachrichtigungsmethode des Administrators über die Ereignisse (beispielsweise SMS, E-Mail-Nachricht)

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignis-Datenverwaltung** die Einstellungen für das Speichern der Ereignisse in der Datenbank des Servers anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Wenn Sie die maximale Anzahl der Ereignisse angeben, berechnet die Anwendung einen ungefähren Wert des für die angegebene Zahl benötigten Speicherplatzes. Sie können diese ungefähre Berechnung verwenden, um zu überprüfen, ob Sie ausreichen freien Platz auf dem Laufwerk haben, um einen Überlauf der Datenbank zu vermeiden. Standardmäßig umfasst die Administrationsserver-Datenbank 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Die Anwendung überprüft die Datenbank alle 10 Minuten. Wenn die Anzahl der Ereignisse den festgelegten Höchstwert plus 10.000 erreicht, löscht die Anwendung die ältesten Ereignisse, sodass nur noch die festgelegte Höchstanzahl von Ereignissen übrig bleibt.

Wenn der Administrationsserver alte Ereignisse löscht, kann er keine neuen Ereignisse in der Datenbank speichern. Während dieser Zeitspanne werden Informationen über abgelehnte Ereignisse in das Kaspersky-Ereignisprotokoll geschrieben. Die neuen Ereignisse werden in die Warteschlange verschoben und dann in der Datenbank gespeichert, nachdem der Löschvorgang abgeschlossen wurde.

Sie können die Einstellungen einer beliebigen Aufgabe ändern, um entweder Ereignisse im Zusammenhang mit dem Aufgabenfortschritt oder nur die Ergebnisse der Aufgabenausführung zu speichern. Auf diese Weise reduzieren Sie die Anzahl der Ereignisse in der Datenbank, erhöhen die Ausführungsgeschwindigkeit der Szenarien, die mit der Analyse der Ereignistabelle in der Datenbank verbunden sind, und reduzieren das Risiko der Verdrängung von kritischen Ereignissen durch eine große Anzahl an Ereignissen.

Protokoll der Verbindungen zum Administrationsserver anzeigen

Der Verlauf der Verbindungen und Versuche, während des Betriebs eine Verbindung mit dem Administrationsserver herzustellen, können in einer Protokolldatei gespeichert werden. Mit den Informationen in der Datei können Sie nicht nur Verbindungen innerhalb Ihrer Netzwerkinfrastruktur verfolgen, sondern auch nicht autorisierte Versuche, auf den Administrationsserver zuzugreifen.

So protokollieren Sie die Ereignisse der Verbindung zum Administrationsserver:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den die Protokollierung der Verbindungsereignisse aktiviert werden soll.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Klicken Sie im folgenden Eigenschaftenfenster im Abschnitt **Verbindungseinstellungen des Administrationsservers** auf den Unterabschnitt **Verbindungsports**.
4. Aktivieren Sie die Option **Verbindungsereignisse des Administrationsservers protokollieren**.
5. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Administrationsservers zu schließen.

Alle weiteren Ereignisse eingehender Verbindungen zum Administrationsserver, Authentifizierungsergebnisse und SSL-Fehler werden in der Datei %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog gespeichert.

Eintreten von Virenangriffen kontrollieren

Mit Kaspersky Security Center können Sie rechtzeitig auf die Bedrohungen von Virenangriffen reagieren. Die Gefahr eines Virenangriffs wird durch die Kontrolle der Virenaktivität auf den Geräten eingeschätzt.

Sie können Regeln zum Einschätzen der Bedrohungen von Virenangriffen und Aktionen, die im Falle eines Virenangriffs ausgeführt werden sollen, im Abschnitt **Virenangriff** des Administrationsserver-Eigenschaftenfensters anpassen.

Die Reihenfolge der Benachrichtigung über das Ereignis *Virenangriff* können Sie im Abschnitt **Konfiguration von Ereignissen** des Eigenschaftenfenster des Administrationsservers im Eigenschaftenfenster des Ereignisses *Virenangriff* bestimmen.

Das Ereignis *Virenangriff* wird bei Eintritt des Ereignisses *Schädliches Objekt gefunden* während der Ausführung der Sicherheitsanwendung gemeldet. Deshalb ist es erforderlich, Informationen über die Ereignisse *Schädliches Objekt gefunden* auf dem Administrationsserver zu speichern, um die Virenangriffe rechtzeitig erkennen zu können.

Die Einstellungen für das Speichern von Informationen über das Ereignis *Schädliches Objekt gefunden* werden in den Richtlinien der Sicherheitsanwendung vorgegeben.

Beim Zählen der Ereignisse *Schädliches Objekt gefunden* werden nur Informationen von den Geräten des primären Administrationsservers berücksichtigt. Informationen von sekundären Administrationsservern werden nicht berücksichtigt. Für jeden sekundären Server müssen die Einstellungen für das Ereignis *Virenangriff* individuell angepasst werden.

Datenverkehr begrenzen

Um den Netzwerkdatenverkehr zu reduzieren, können Sie die Geschwindigkeit der Datenübertragung von einzelnen IP-Bereichen und IP-Intervallen an den Administrationsserver einschränken.

Sie können Regeln für die Einschränkung des Datenverkehrs im Abschnitt **Datenverkehr** des Administrationsserver-Eigenschaftenfensters erstellen und anpassen.

Gehen Sie folgendermaßen vor, um eine Regel zu Begrenzung des Datenverkehrs zu erstellen:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des Administrationsservers aus, für Sie eine Regel zur Begrenzung des Datenverkehrs erstellen möchten.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Datenverkehr** aus.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.
5. Geben Sie in dem Fenster **Neue Regel** die folgenden Einstellungen an:

Im Block **IP-Intervall, für welchen der Datenverkehr eingeschränkt werden soll** können Sie eine Methode für die Eingabe des Subnetzes oder des Bereiches auswählen, für das bzw. den die Geschwindigkeit der Datenübertragung beschränkt werden muss. Außerdem können Sie die Einstellungen für die ausgewählte Methode konfigurieren. Wählen Sie eine der folgenden Methoden aus:

- **Bereich mittels Adresse und Netzwerkmaske eingeben**

  Der Datenverkehr wird entsprechend den Einstellungen des Subnetzes begrenzt. Geben Sie die Subnetzadresse und die Subnetzmaske zur Bestimmung des Bereichs, in dem der Datenverkehr begrenzt werden soll, an.

  Sie können auch auf **Durchsuchen** klicken, um Subnetze aus der globalen Liste der Subnetze hinzufügen.

- **Bereich mittels Start- und End-Adressen angeben**

  Der Datenverkehr wird entsprechend den Intervallen der IP-Adressen begrenzt. Geben Sie in den Eingabefeldern **Anfang** und **Ende** den Bereich von IP-Adressen an.

  Diese Variante ist standardmäßig festgelegt.

Im Abschnitt **Einschränkung für Datenverkehr** können Sie die folgenden Beschränkungseinstellungen für die Geschwindigkeit der Datenübertragung konfigurieren:

- **Zeitintervall**

  Zeitraum, in dem die Beschränkung des Datenverkehrs gelten soll. Die Grenzwerte für den Zeitraum sind in den Eingabefeldern einzugeben.

- **Einschränkung (KB/Sek.)**

  Kritischer Wert für die Gesamtübertragungsrate der eingehenden und ausgehenden Daten des Administrationsservers. Die Beschränkung soll nur innerhalb des Zeitraums gelten, der im Feld **Zeitraum** vorgegeben wurde.

- **Datenverkehr in der übrigen Zeit einschränken (KB/s)**

  Der Datenverkehr wird nicht nur innerhalb des im Feld **Zeitraum** eingegebenen Zeitraums beschränkt, sondern auch in der übrigen Zeit.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert. Der Wert des Feldes darf nicht mit dem Wert des Felds **Einschränkung (KB/Sek.)** übereinstimmen.

In erster Linie betreffen Regeln zur Einschränkung für Datenverkehr die Übertragung von Dateien. Diese Regeln werden nicht für den Datenverkehr übernommen, der mittels Synchronisierung zwischen Administrationsserver und Administrationsagent oder zwischen dem primären und den sekundären Administrationsservern erzeugt wird.

Webserver-Einstellungen anpassen

Der Webserver ermöglicht die Veröffentlichung von autonomen Installationspaketen, iOS MDM-Profilen sowie Dateien aus dem freigegebenen Ordner.

Sie können die Einstellungen für die Verbindung des Webservers mit dem Administrationsserver anpassen und das Webserver-Zertifikat im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers festlegen.

Arbeit mit internen Benutzern

Die Benutzerkonten der *internen Benutzer* werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Innerhalb der Funktionen von Kaspersky Security Center verfügen die internen Benutzer über die Berechtigungen tatsächlicher Benutzer.

Benutzerkonten der internen Benutzer werden nur innerhalb von Kaspersky Security Center erstellt und verwendet. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center.

Sie können die Benutzerkonto-Einstellungen für interne Benutzer im Ordner **Benutzerkonten** der Konsolenstruktur anpassen.

Verschieben ins Backup und Wiederherstellen der Einstellungen des Administrationsservers

Für das Verschieben der Einstellungen des Administrationsservers und der von ihm verwendeten Datenbank ins Backup ist die Aufgabe zum Verschieben ins Backup und das Tool klbackup vorgesehen. Die Backup-Kopie umfasst alle Haupteinstellungen und Objekte des Administrationsservers: die Zertifikate des Administrationsservers, die Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte, die Lizenzschlüssel, die Struktur der Administrationsgruppen mit sämtlichem Inhalt, die Aufgaben, die Richtlinien und mehr. Mit einer Backup-Kopie kann die Funktionsfähigkeit eines Administrationsservers schnellstmöglich wiederhergestellt werden, was wenige Minuten oder bis zu zwei Stunden dauern kann.

Bei einer fehlenden Backup-Kopie kann eine Störung zum unwiederbringlichen Verlust der Zertifikate und aller Einstellungen des Administrationsservers führen. Kaspersky Security Center muss dann erneut konfiguriert werden und die erstmalige Bereitstellung des Administrationsagenten im Netzwerk des Unternehmens muss erneut ausgeführt werden. Außerdem gehen auch alle Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte verloren, was das Risiko eines unwiederbringlichen Verlustes der verschlüsselten Daten auf den Geräten mit Kaspersky Endpoint Security mit sich bringt. Auf das regelmäßige Erstellen von Backup-Kopien des Administrationsservers mithilfe der Standardaufgabe zum Verschieben ins Backup darf keinesfalls verzichtet werden.

Der Schnellstartassistent erstellt die Aufgabe zum Anlegen eines Backups der Einstellungen des Administrationsservers mit einem täglichen Start um 4:00 Uhr morgens. Gespeichert werden die Backup-Kopien standardmäßig im Ordner %ALLUSERSPROFILE%\Application Data\KasperskySC.

Wenn als DBMS ein Instanz von Microsoft SQL Server, die auf einem anderen Gerät installiert ist, verwendet wird, muss die Aufgabe zum Verschieben ins Backup geändert werden: als Ordner für die Speicherung der erstellten Backup-Kopien muss der UNC-Pfad angegeben werden, der sowohl als Dienst des Administrationsservers als auch als Dienst für SQL Server für einen Eintrag verfügbar ist. Diese Anforderung ist eine Folge der Untersuchung des Verschiebens ins Backup im DBMS Microsoft SQL Server.

Wenn als DBMS eine lokale Instanz von Microsoft SQL Server verwendet wird, empfehlen wir außerdem, die Backup-Kopien auf einem separaten Datenträger zu speichern, um sie gleichzeitig mit dem Administrationsserver vor Beschädigung zu sichern.

Da eine Backup-Kopie wichtige Daten enthält, ist in der Aufgabe zum Verschieben ins Backup und im Tool klbackup der Schutz der Backup-Kopien durch ein Kennwort vorgesehen. Standardmäßig wird die Aufgabe zum Verschieben ins Backup mit einem leeren Kennwort erstellt. Das Kennwort muss in den Eigenschaften der Aufgabe zum Verschieben ins Backup unbedingt festgelegt werden. Wenn diese Forderung nicht erfüllt wird, führt das dazu, dass die Schlüssel der Zertifikate des Administrationsservers, die Schlüssel für die Lizenzen und die Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte nicht verschlüsselt sind.

Neben dem regelmäßigen Verschieben ins Backup muss auch eine Backup-Kopie aller wichtiger Änderungen erstellt werden, darunter auch vor dem Update des Administrationsservers auf die neue Version und vor der Installation der Patches des Administrationsservers.

Wenn Sie Microsoft SQL Server als DBMS verwenden, können Sie die Größe der Sicherungskopien minimieren. Um dies zu tun, aktivieren Sie das Kontrollkästchen **Backup komprimieren** (Compress backup) in den SQL Server-Einstellungen.

Die Wiederherstellung aus der Backup-Kopie wird mithilfe des Tools klbackup mit der gerade erst installierten und funktionsfähigen Instanz des Administrationsservers jener Version durchgeführt, für die eine Backup-Kopie erstellt wurde (oder neuer).

Die Instanz des Administrationsservers, auf der die Wiederherstellung ausgeführt werden soll, muss ein DBMS desselben Typs (z. B. der gleiche SQL Server oder MariaDB) und derselben Version oder höher verwenden. Die Version des Administrationsservers kann gleich (mit einem ähnlichen oder neueren Patch) oder neuer sein.

In diesem Abschnitt werden typische Szenarien für die Wiederherstellung der Einstellungen und der Objekte des Administrationsservers beschrieben.

Nutzung von Momentaufnahmen des Dateisystems zur Verkürzung der Dauer des Verschiebens ins Backup

In Kaspersky Security Center 15.1 wurde im Vergleich zu früheren Versionen die Leerlaufzeit des Administrationsservers während des Verschiebens von Daten in Backup verringert. Außerdem wurde in den Einstellungen der Aufgabe die Funktion **Bei Anlegen eines Daten-Backups Snapshot des Dateisystems benutzen** hinzugefügt. Diese Funktion erlaubt eine weitere Verkürzung der Leerlaufzeit, indem das Tool klbackup beim Verschieben ins Backup eine Schattenkopie des Laufwerks erstellt (was einige Sekunden dauert) und gleichzeitig ein Kopieren der Datenbank erfolgt (was nicht mehr als einige Minuten in Anspruch nimmt). Nach dem Erstellen einer Schattenkopie des Laufwerks und dem Kopieren der Datenbank macht klbackup den Administrationsserver wieder für Verbindungen verfügbar.

Sie können die Funktion zum Erstellen einer Momentaufnahme des Dateisystems nur bei Beachtung von zwei Bedingungen benutzen:

- Der freigegebene Ordner des Administrationsservers und der Ordner %ALLUSERSPROFILE%\KasperskyLab befinden sich auf einem logischen Laufwerk und sind lokal in Bezug auf den Administrationsserver.
- Innerhalb des Ordners %ALLUSERSPROFILE%\KasperskyLab gibt es keine manuell erstellten symbolischen Links.

Verwenden Sie die Funktion nicht, wenn mindestens eine dieser Bedingungen nicht erfüllt wird. Als Antwort auf den Versuch, eine Momentaufnahme des Dateisystems des Programms zu erstellen wird eine Fehlermeldung ausgegeben.

Für die Nutzung der Funktion muss ein Benutzerkonto mit Berechtigungen zum Erstellen von Momentaufnahmen des logischen Laufwerks verfügbar sein, auf dem sich der Ordner %ALLUSERSPROFILE% befindet. Das Benutzerkonto für Dienst des Administrationsservers verfügt nicht über solche Rechte.

Um die Funktion zum Erstellen von Momentaufnahmen des Dateisystems zur Verkürzung der Zeit für das Verschieben ins Backup zu nutzen, gehen Sie wie folgt vor:

1. Wählen Sie im Abschnitt **Aufgaben** die Aufgabe zum Verschieben ins Backup aus.
2. Wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.
3. Wählen Sie im nächsten Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
4. Aktivieren Sie das Kontrollkästchen **Bei Anlegen eines Daten-Backups Snapshot des Dateisystems benutzen**.
5. Geben Sie in den Feldern **Benutzername** und **Kennwort** den Namen und das Kennwort des Benutzerkontos ein, das über Berechtigungen zum Erstellen von Momentaufnahmen des logischen Laufwerks verfügt, auf dem sich der Ordner %ALLUSERSPROFILE% befindet.
6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Bei den folgenden Starts der Aufgabe zum Verschieben ins Backup erstellt das Tool klbackup Momentaufnahmen des Dateisystems und die Leerlaufzeit des Administrationsservers während der Ausführung der Aufgabe wird verringert.

Ein Gerät mit dem Administrationsserver ist ausgefallen

Wenn das Gerät mit dem Administrationsserver infolge einer Störung außer Betrieb ist, wird empfohlen, wie folgt vorzugehen:

- Dem neuen Administrationsserver dieselbe Adresse zuweisen: NetBIOS-Name, FQDN-Name, statische IP-Adresse, wobei berücksichtigt werden muss, was bei der Bereitstellung des Administrationsagenten festgelegt wurde.
- Administrationsserver unter Verwendung eines DBMS desselben Typs und derselben oder einer neueren Version installieren. Es kann dieselbe Version des Servers mit demselben oder einem neueren Patch, oder eine neuere Version installiert werden. Nach der Installation muss keine Erstkonfiguration mithilfe des Assistenten ausgeführt werden.
- Starten Sie im Menü **Start** das Tool "klbackup" und führen Sie die Wiederherstellung durch.

Die Einstellungen des Administrationsservers oder der Datenbank sind beschädigt

Wenn der Administrationsserver infolge der Beschädigung der Einstellungen oder der Datenbank funktionsunfähig wurde (beispielsweise wegen eines Stromausfalls), wird empfohlen, das folgende Szenario für die Wiederherstellung zu verwenden:

1. Untersuchung des Dateisystems auf dem betroffenen Gerät durchführen.
2. Funktionsunfähige Version des Administrationsservers deinstallieren.

3. Administrationsserver unter Verwendung eines DBMS desselben Typs und derselben oder einer neueren Version erneut installieren. Es kann dieselbe Version des Servers mit demselben oder einem neueren Patch, oder eine neuere Version installiert werden. Nach der Installation muss keine Erstkonfiguration mithilfe des Assistenten ausgeführt werden.

4. Das Sicherungs- u. Wiederherstellungstool klbackup aus dem Menü **Start** ausführen und die Wiederherstellung ausführen.

Es ist unmöglich, den Administrationsserver auf andere Weise als mit dem Standardtool klbackup wiederherzustellen.

In sämtlichen Fälle der Wiederherstellung des Administrationsservers mithilfe von Drittanbieter-Programmen kommt es unvermeidlich zu einer Desynchronisierung der Daten in den Knoten des verteilten Programms Kaspersky Security Center und in der Folge zu einer inkorrekten Ausführung des Programms.

Backup-Kopie der Daten des Administrationsservers anlegen und wiederherstellen

Ein Daten-Backup ermöglicht es Ihnen, den Administrationsserver ohne Datenverlust von einem Gerät auf ein anderes zu übertragen. Mittels eines Backups können Sie Daten wiederherstellen, wenn Sie die Administrationsserver-Datenbank auf ein anderes Gerät verschieben oder auf eine aktuellere Version von Kaspersky Security Center aktualisieren. Darüber hinaus erlaubt die Verwendung eines Daten-Backups das Verschieben der Daten des Administrationsservers von Kaspersky Security Center Windows unter die Verwaltung von Kaspersky Security Center Linux (ein Verschieben der Daten von Kaspersky Security Center Linux zu Kaspersky Security Center Windows wird nicht unterstützt).

Die installierten Verwaltungs-Plug-ins werden nicht mittels Backup gesichert. Nachdem Sie die Daten des Administrationsservers aus einer Sicherungskopie wiederhergestellt haben, müssen Sie Plug-ins für die verwalteten Anwendungen herunterladen und neu installieren.

Bevor Sie ein Backup des Administrationsservers erstellen, prüfen Sie, ob ein virtueller Administrationsserver zur Administrationsgruppe hinzugefügt wurde. Sollte ein virtueller Administrationsserver hinzugefügt worden sein, stellen Sie vor dem Backup sicher, dass dem virtuellen Administrationsserver ein Administrator zugewiesen ist. Nach dem Backup können Sie für den virtuellen Administrationsserver keine Administratorrechte mehr vergeben. Beachten Sie, dass im Sie im Falle des Verlusts der Anmeldeinformationen des Administrators nicht mehr in der Lage sind, dem virtuellen Administrationsserver einen neuen Administrator zuzuweisen.

Um einen Failover-Cluster für Kaspersky Security Center zu sichern oder wiederherzustellen, müssen Sie den gesamten Cluster zu Wartungszwecken anhalten und ihn nach Abschluss der Sicherung oder Wiederherstellung neu starten.

Sie können eine Backup-Kopie der Daten des Administrationsservers auf eine der folgenden Weisen erstellen:

- Eine Aufgabe zum Anlegen eines Daten-Backups über die Verwaltungskonsole erstellen und starten.
- Das Tool klbackup auf einem Gerät mit dem installierten Administrationsserver starten. Dieses Tool gehört zum Lieferumfang von Kaspersky Security Center. Es befindet sich nach der Installation des Administrationsservers im Stammverzeichnis des Zielordners, der bei der Installation angegeben wurde.

In der Backup-Kopie der Daten des Administrationsservers werden folgende Daten gespeichert:

- Administrationsserver-Datenbank (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse).
- Konfigurationsdaten über die Struktur der Administrationsgruppen und Client-Geräte.
- Speicherort der Programmpakete für die Remote-Installation.
- Zertifikat des Administrationsservers.
- Inhalt des Ordners *Updates*.

  Der Ordnerpfad lautet standardmäßig C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Die Wiederherstellung von Daten des Administrationsservers ist nur mithilfe des Hilfsprogramms klbackup möglich. Sie müssen die Wiederherstellung auf einer funktionierenden Instanz des Administrationsservers durchführen, die gerade installiert wurde und die gleiche Version (oder höher) besitzt, für welche die Sicherung erstellt wurde.

Aufgabe zum Anlegen eines Backups der Daten des Administrationsservers

Erstellen einer Aufgabe zum Anlegen eines Backups der Daten des Administrationsservers

Die Backup-Aufgabe ist eine Aufgabe des Administrationsservers und über den Schnellstartassistenten erstellt. Wenn die vom Schnellstartassistenten erstellte Aufgabe zum Anlegen eines Backups gelöscht wurde, können Sie diese manuell erstellen.

So erstellen Sie eine Aufgabe zum Anlegen eines Backups der Daten des Administrationsservers:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Weisen:
   - Wählen Sie in der Konsolenstruktur aus dem Kontextmenü des Ordners **Aufgaben** den Punkt **Neu** → **Aufgabe** aus.
   - Klicken Sie auf die Schaltfläche **Aufgabe erstellen** im Arbeitsbereich.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten den Aufgabentyp **Backup der Daten des Administrationsservers anlegen** aus.

Die Aufgabe **Backup der Daten des Administrationsservers anlegen** kann nur einmal erstellt werden. Wenn die Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers für den Administrationsserver bereits erstellt wurde, wird sie im Fenster für die Auswahl des Aufgabentyps des Assistenten für das Erstellen einer Aufgabe zum Anlegen eines Backups nicht angezeigt.

Aufgabe zum Anlegen eines Backups der Daten des Administrationsservers konfigurieren

Nach dem Erstellen einer Backup-Aufgabe, können Sie die Einstellungen der Aufgabe anpassen.

So konfigurieren Sie die Aufgabe Backup der Daten des Administrationsservers anlegen:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Wählen Sie im Kontextmenü der Aufgabe **Backup der Daten des Administrationsservers anlegen** die Option **Eigenschaften** aus.

Das Fenster mit den Einstellungen der Aufgabe *Backup der Daten des Administrationsservers anlegen* wird geöffnet. Die folgenden Einstellungen verfügbar:

- **Allgemein**

  Im Abschnitt **Allgemein** können Sie den Aufgabennamen angeben und folgende Informationen anzeigen: das Erstellungsdatum der Aufgabe, das Datum des letzten Befehls, den Status des Aufgabenstarts und die Aufgabenergebnisse.

- **Benachrichtigung**

  Im Abschnitt **Benachrichtigung** können Sie die Einstellungen für das Speichern von Ereignissen, die sich auf die Aufgabenausführung beziehen, sowie von Aufgaben festlegen. Außerdem können Sie die Benachrichtigungen über die Ergebnisse der Aufgabenausführung anpassen.

- **Zeitplan**

  Im Abschnitt **Zeitplan** können Sie einen Zeitplan für den Aufgabenstart festlegen.

- **Ziel**

  Im Abschnitt **Ziel** können Sie den Pfad des Ordners angeben, in dem die Backup-Kopien der Daten des Administrationsservers gespeichert werden sollen.

- **Einstellungen**

  Im Abschnitt **Einstellungen** können Sie bei Bedarf das Kennwort zum Schutz des Backups und die Anzahl der zu erstellenden Backup-Kopien festlegen.

  Sie können außerdem eine Schattenkopie des logischen Datenträgers erstellen, auf dem der Ordner "%ALLUSERSPROFILE%" gespeichert ist, und die Datenbank des Administrationsservers kopieren. Dazu müssen Sie die Option **Snapshot des Dateisystems für Datei-Backup verwenden** aktivieren und den Namen und das Kennwort eines Benutzerkontos angeben, das über die Berechtigung zum Erstellen von Snapshots verfügt.

- **Sicherheit**

  Im Abschnitt **Sicherheit** können Sie Benutzern und Gruppen Berechtigungen zum Ausführen von Vorgängen auf dem Administrationsserver erteilen. Wenn die Option **Einstellungen vom Administrationsserver erben** aktiviert ist, werden die Sicherheitseinstellungen für die Aufgabe vom Administrationsserver übernommen.

  Wenn diese Option deaktiviert ist, können Sie Sicherheitseinstellungen für die Aufgabe anpassen. Zuweisen können einem Benutzer oder einer Gruppe von Benutzern entweder eine Rolle oder die gleichen Berechtigungen, wie sie der Aufgabe zugewiesen sind.

  Standardmäßig ist die Option **Einstellungen vom Administrationsserver erben** aktiviert.

- **Revisionsverlauf**

  Im Abschnitt **Revisionsverlauf** können Sie die Änderung der Aufgabeneinstellungen nachverfolgen. Jedes Mal, wenn Sie die Änderungen der Aufgabe speichern, wird eine Revision erstellt.

Tool zur Sicherung- und Wiederherstellung der Daten (klbackup)

Sie können die Daten des Administrationsservers mittels des Tools "klbackup", welches im Lieferumfang von Kaspersky Security Center enthalten ist, zum Zweck eines Backups und späterer Wiederherstellung kopieren.

Das Tool "klbackup" kann in zwei Modi arbeiten:

- Interaktiv
- Lautlos (Silent)

Daten im interaktiven Modus sichern, kopieren und wiederherstellen

Beim Wiederherstellen der Administrationsserverdaten aus einer Backup-Kopie, die mit dem Tool "klbackup" im interaktiven Modus erstellt wurde, kann ein Fehler auftreten. Wenn Sie den Patch 15.1.0.20748-pf2 für den Administrationsserver installiert haben und anschließend mittels des Tools "klbackup" bei deaktivierter Option **Datenbank migrieren** eine Backup-Kopie erstellen, tritt beim Wiederherstellen dieser Kopie ein Fehler auf (Betrifft alle DBMS außer MySQL und MariaDB). Wenn Sie den Patch 15.1.0.20748-pf2 für den Administrationsserver installiert haben und eine Backup-Kopie erstellen möchten, ohne auf ein anderes DBMS zu migrieren, verwenden Sie eine Aufgabe zum Erstellen eines Daten-Backups oder führen Sie das Tool "klbackup" über die Befehlszeile aus.

Um eine Backup-Kopie der Daten des Administrationsservers im interaktiven Modus zu erstellen, gehen Sie wie folgt vor:

1. Tool klbackup ausführen, das sich im Installationsordner von Kaspersky Security Center befindet.

   Der Backup- und Wiederherstellungsassistent wird gestartet.

2. Wählen Sie im ersten Fenster des Assistenten die Option **Anlegen eines Backups der Daten des Administrationsservers** aus.

   Bei aktivierter Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** wird nur eine Backup-Kopie des Zertifikats des Administrationsservers und des privaten Schlüssels gespeichert. Eine Backup-Kopie vom Zertifikat des Administrationsservers und vom privaten Schlüssel kann nützlich sein, wenn Sie vom Kaspersky Security Center Administrationsserver auf den Administrationsserver von Kaspersky Security Center Linux migrieren. Darüber hinaus können Sie sowohl verwaltete Geräte zwischen Administrationsservern von Kaspersky Security Center Linux als auch verwaltete Geräte zwischen Administrationsservern von Kaspersky Security Center Windows migrieren. Weitere Informationen dazu finden Sie unter Verwenden des klbackup-Tools, um verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers zu stellen.

   Klicken Sie auf die Schaltfläche **Weiter**.

3. Geben Sie im nächsten Fenster des Assistenten die folgenden Optionen an:

- **Zielordner des Backups**
- **Datenbank migrieren**

  Aktivieren Sie diese Option, wenn Sie Daten des Administrationsservers aktuell in einer Microsoft SQL Server-Datenbank speichern und Sie diese auf eine der folgenden Datenbanken migrieren möchten: MySQL oder MariaDB, PostgreSQL oder Postgres Pro, Azure SQL. Diese Option ist standardmäßig deaktiviert.

  - **Auf MySQL/MariaDB-Format migrieren**

    Aktivieren Sie diese Option, wenn Sie derzeit SQL Server als DBMS für den Administrationsserver verwenden und die Daten von SQL Server zu MySQL oder MariaDB DBMS migrieren möchten. Kaspersky Security Center erstellt ein mit MySQL und MariaDB kompatibles Backup. Danach können Sie die Daten aus dem Backup in MySQL oder MariaDB wiederherstellen.

  - **Auf Postgres migrieren**

    Aktivieren Sie diese Option, wenn Sie derzeit SQL Server als DBMS für den Administrationsserver verwenden und die Daten von SQL Server zu PostgreSQL oder Postgres Pro DBMS migrieren möchten. Kaspersky Security Center erstellt ein mit PostgreSQL und Postgres Pro kompatibles Backup. Danach können Sie die Daten aus dem Backup in PostgreSQL oder Postgres Pro wiederherstellen.

    Diese Option wird verfügbar, wenn Sie beim Technischen Support von Kaspersky den Patch 15.1.0.20748-pf2 für den Administrationsserver anfragen und anschließend installieren, oder wenn Sie Kaspersky Security Center Windows auf die Version 15.1.0.22239 aktualisieren.

  - **Auf Azure-Format migrieren**

    Aktivieren Sie diese Option, wenn Sie derzeit SQL Server als DBMS für den Administrationsserver verwenden und die Daten von SQL Server zu Azure SQL DBMS migrieren möchten. Kaspersky Security Center erstellt ein mit Azure SQL kompatibles Backup. Danach können Sie die Daten aus dem Backup in Azure SQL wiederherstellen.

- **Aktuelles Datum mit Uhrzeit zum Namen des Backup-Zielordners hinzufügen**
- **Kennwort für das Backup**

4. Klicken Sie auf **Weiter**, um das Verschieben ins Backup zu starten.

5. Wenn Sie mit einer Datenbank in einer Cloud-Umgebung wie Amazon Web Services (AWS) oder Microsoft Azure arbeiten, füllen Sie bitte im Fenster **Bei Cloud-Speicher anmelden** die folgenden Felder aus:

   - Für AWS:

     - **Name des S3-Buckets**

       Name des S3-Buckets, den Sie für das Backup erstellt haben.

     - **ID des Zugriffsschlüssels**

       Sie haben die Schlüssel-ID (Abfolge von alphanumerischen Zeichen) erhalten, als Sie das IAM-Benutzerkonto erstellt haben, um mit der Speicher-Instanz des S3-Buckets zu arbeiten.

       Dieses Feld ist verfügbar, wenn Sie RDS-Datenbank auf einem S3-Bucket ausgewählt haben.

- **Geheimer Schlüssel**

  Geheimer Schlüssel, den Sie gemeinsam mit der ID des Zugriffsschlüssels erhalten haben, als Sie das IAM-Benutzerkonto erstellt haben.

  Die Zeichen des geheimen Schlüssels werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des geheimen Schlüssels begonnen haben, wird die Schaltfläche **Anzeigen** angezeigt. Klicken Sie auf diese Schaltfläche und halten Sie diese so lange wie nötig gedrückt, um die eingegebenen Zeichen anzuzeigen.

  Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

- Für Microsoft Azure:

  - **Name des Azure-Speicherkontos**

    Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

  - **Azure-Abonnement-ID**

    Sie haben das Abonnement auf dem Azure-Portal erstellt.

  - **Azure-Kennwort**

    Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

    Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

  - **Anwendungs-ID für Azure**

    Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

    Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

  - **Name des Azure SQL-Servers**

    Der Name und die Gruppe der Ressourcen sind in den Eigenschaften Ihres Azure SQL-Servers verfügbar.

  - **Azure SQL-Serverressourcengruppe**

    Der Name und die Gruppe der Ressourcen sind in den Eigenschaften Ihres Azure SQL-Servers verfügbar.

  - **Zugriffsschlüssel für Azure-Speicher**

    Verfügbar in den Eigenschaften Ihres Speicherkontos im Abschnitt "Zugriffsschlüssel". Sie können einen der Schlüssel (Schlüssel1 oder Schlüssel2) verwenden.

Um Daten des Administrationsservers im interaktiven Modus wiederherzustellen, gehen Sie wie folgt vor:

1. Tool klbackup ausführen, das sich im Installationsordner von Kaspersky Security Center befindet. Starten Sie das Tool unter demselben Benutzerkonto, mit dem Sie auch den Administrationsserver installiert haben. Wir empfehlen, das Tool auf einem neu installierten Administrationsserver auszuführen.

   Der Backup- und Wiederherstellungsassistent wird gestartet.

2. Wählen Sie im ersten Fenster des Assistenten die Option **Wiederherstellen der Daten des Administrationsservers** aus und klicken Sie anschließend auf **Weiter**.

   Wenn Sie die Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** auswählen, wird nur das Zertifikat des Administrationsservers und des privaten Schlüssels wiederhergestellt.

   Wenn Sie das Tool "klbackup" auf dem inaktiven Konten eines Failover-Clusters ausführen, werden Sie aufgefordert, eine der folgenden Optionen auszuwählen: Zertifikat des Administrationsservers angeben oder Daten automatisch vom Administrationsserver abrufen.

3. Gehen Sie im Assistenten im Fenster **Einstellungen für Wiederherstellung** folgendermaßen vor:

   - Geben Sie den Ordner an, der die Backup-Kopie der Daten des Administrationsservers enthält.

     Wenn Sie in einer Cloud-Umgebung wie AWS oder Azure arbeiten, geben Sie die Adresse des Speichers an. Stellen Sie außerdem sicher, dass die Datei backup.zip heißt.

   - Geben Sie das Kennwort ein, das beim Anlegen des Daten-Backups festgelegt wurde.

     Beim Wiederherstellen der Daten muss dasselbe Kennwort eingegeben werden wie beim Verschieben ins Backup. Wenn der Pfad zum freigegebenen Ordner nach dem Verschieben ins Backup verändert wird, muss nach der Wiederherstellung der Daten die Funktion jener Aufgaben überprüft werden, bei denen die wiederhergestellten Daten verwendet werden (Wiederherstellungsaufgaben, Remote-Installation). Erforderlichenfalls müssen die Einstellungen dieser Aufgaben geändert werden. Während der Wiederherstellung von Daten aus dem Backup darf der freigegebene Ordner des Administrationsservers von niemandem verwendet werden. Das Benutzerkonto, unter dem das Tool klbackup gestartet wird, muss über vollen Zugriff auf den freigegebenen Ordner verfügen.

4. Klicken Sie auf die Schaltfläche **Weiter** für die Wiederherstellung von Daten.

Daten im Silent-Modus sichern, kopieren und wiederherstellen

So erstellen Sie eine Backup-Kopie der Daten oder stellen die Daten des Administrationsservers im Silent-Modus wieder her:

Starten Sie aus der Befehlszeile des Geräts, auf dem der Administrationsserver installiert ist, das Tool klbackup mit der erforderlichen Auswahl an Schlüsseln.

Bei Verwendung des Tools "klbackup" werden die Flags des Administrationsagenten nicht wiederhergestellt. Sie müssen die Flags des Administrationsagenten manuell konfigurieren.

Die Instanz des Administrationsservers, auf der die Wiederherstellung ausgeführt werden soll, muss ein DBMS desselben Typs verwenden. Die Version des Administrationsservers kann gleich (mit einem ähnlichen oder neueren Patch) oder neuer sein.

Die Befehlszeilensyntax des Tools lautet:

```
klbackup -path <backup path> [-linux_path < Backup-Pfad des SQL Servers >][-node_cert
< Zertifikat-Pfad >] [-logfile < Protokollfdatei >] [-use_ts]|[-restore] [-password
< Kennwort >] [-cert_only] [-online] [-migrate postgres]
```

Wenn in der Befehlszeile des Tools klbackup kein Kennwort eingegeben wird, fragt das Tool das Kennwort interaktiv ab.

Beschreibung der Parameter:

- `-path <Backup-Pfad>` – Daten im angegebenen Backup-Ordner speichern bzw. aus dem Backup-Ordner wiederherstellen (Pflichtparameter).

  Das Benutzerkonto der Server-Datenbank und das klbackup-Tool müssen über die Berechtigung zum Ändern der Daten im Backup-Ordner verfügen.

- `-linux_path <Backup-Pfad des SQL-Servers>` – Lokaler Pfad des Ordners mit den Backup-Daten für SQL Server unter Linux.

  Das Benutzerkonto der Server-Datenbank und das klbackup-Tool müssen über die Berechtigung zum Ändern der Daten im Backup-Ordner des SQL-Servers verfügen.

- `-node_cert <Zertifikat-Pfad>` – Server-Zertifikatsdatei zum Konfigurieren inaktiver Failover-Cluster-Knoten nach der Wiederherstellung. Wenn kein Pfad festgelegt ist, wird er automatisch vom Server abgerufen.

  Wenn Sie das Tool klbackup auf dem inaktiven Knoten Failover-Clusters ausführen, verwenden Sie diesen Schlüssel, um den Pfad zum Serverzertifikat anzugeben.

- `-logfile <Log-Datei>` – Bericht über das Anlegen und Wiederherstellen eines Daten-Backups des Administrationsservers speichern.

- `-use_ts` – Kopiert beim Speichern die Informationen in einen Unterordner des Backup-Ordners, wobei der Name des Unterordners im Format `klbackup YYYY-MM-DD # HH-MM-SS` angegeben ist und die aktuelle UTC-Zeit enthält. Wenn der Schlüssel nicht eingegeben wurde, werden die Angaben im Stammverzeichnis des Backup-Ordners abgelegt.

  Wenn Sie versuchen, die Informationen in einem Ordner zu speichern, in dem bereits eine Backup-Kopie vorhanden ist, erscheint eine Fehlermeldung. Die Informationen werden nicht aktualisiert.

  Mit dem Schlüssel `-use_ts` kann ein Datenarchiv des Administrationsservers angelegt werden. Wenn z. B. mit dem Schlüssel `-path` der Ordner `C:\KLBackups` vorgegeben wurde, werden im Ordner `klbackup 2022/6/19 # 11-30-18` Informationen über den Status des Administrationsservers mit Stand vom 19. Juni 2022 um 11 Uhr, 30 Minuten und 18 Sekunden abgelegt.

- `-restore` – Daten des Administrationsservers wiederherstellen. Die Wiederherstellung der Daten erfolgt anhand der Informationen, die sich im Backup-Ordner befinden. Wenn kein Schlüssel vorhanden ist, werden die Daten im Backup-Ordner gesichert.

- `-password <Kennwort>` – Kennwort zum Schutz der vertraulichen Daten.

  > Ein vergessenes Kennwort kann nicht wiederhergestellt werden. Es gibt keine Kennwortanforderungen. Die Kennwortlänge ist unbegrenzt und eine Länge von Null (kein Kennwort) ist ebenfalls möglich.

  Beim Wiederherstellen der Daten muss dasselbe Kennwort eingegeben werden wie beim Verschieben ins Backup. Wenn der Pfad zum freigegebenen Ordner nach dem Verschieben ins Backup verändert wird, muss nach der Wiederherstellung der Daten die Funktion jener Aufgaben überprüft werden, bei denen die wiederhergestellten Daten verwendet werden (Wiederherstellungsaufgaben, Remote-Installation). Erforderlichenfalls müssen die Einstellungen dieser Aufgaben geändert werden. Während der Wiederherstellung von Daten aus dem Backup darf der freigegebene Ordner des Administrationsservers von niemandem verwendet werden. Das Benutzerkonto, unter dem das Tool klbackup gestartet wird, muss über vollen Zugriff auf den freigegebenen Ordner verfügen. Wir empfehlen, das Tool auf einem neu installierten Administrationsserver auszuführen.

- `-cert_only` – Nur das Zertifikat und den privaten Schlüssel des Administrationsservers speichern oder wiederherstellen.

  Dieses Flag kann nützlich sein, wenn Sie eine Migration von einem Administrationsserver für Kaspersky Security Center Windows auf einen Administrationsserver für Kaspersky Security Center Linux durchführen. Darüber hinaus erlaubt es die Migration verwalteter Geräte zwischen Administrationsservern von Kaspersky Security Center Linux sowie zwischen Administrationsservern von Kaspersky Security Center Windows.

- `-online` – Daten des Administrationsservers mithilfe der Erstellung eines Volume-Snapshots sichern, um die Offline-Zeit des Administrationsservers zu reduzieren. Wenn Sie das Tool zur Wiederherstellung von Daten verwenden, wird diese Option ignoriert. Verwenden Sie dieses Flag nicht, wenn Sie ein Backup erstellen, um zu einem anderen DBMS zu migrieren.

- `-archive 0` – Serverdaten als einfache Dateien speichern. Standardmäßig (`[[-archive 1]] 1`) werden die Serverdaten in einer Archivdatei gespeichert.

- `-migrate mysql` – Das Backup der in der SQL Server-Datenbank gespeicherten Daten wird mit Kompatibilität zu MySQL (inkl. MariaDB) erstellt. Sie können die Backup-Daten in MySQL wiederherstellen.

- `-migrate postgres` – Erstellen einer Backup-Kopie der in der SQL Server-Datenbank gespeicherten Administrationsserver-Daten. Das Backup ist anschließend kompatibel zu PostgreSQL und Postgres Pro. Sie können die Daten des Backups in PostgreSQL oder Postgres Pro wiederherstellen. Verwenden Sie dieses Flag, wenn Sie die Migration zu Kaspersky Security Center Linux mithilfe eines Backups der Administrationsserver-Daten durchführen.

  Diese Option wird verfügbar, wenn Sie beim Technischen Support von Kaspersky den Patch 15.1.0.20748-pf2 für den Administrationsserver anfragen und anschließend installieren, oder wenn Sie Kaspersky Security Center Windows auf die Version 15.1.0.22239 aktualisieren.

Das klbackup-Tool verwenden, um verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers zu stellen

Mit dem Tool klbackup können Sie verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers stellen. Mit dem klbackup-Tool können Sie im Rahmen einer Migration vom Administrationsserver für Kaspersky Security Center Windows auf einen Administrationsserver für Kaspersky Security Center Linux wechseln. Darüber hinaus können Sie sowohl verwaltete Geräte zwischen Administrationsservern von Kaspersky Security Center Linux als auch verwaltete Geräte zwischen Administrationsservern von Kaspersky Security Center Windows migrieren.

So stellen Sie verwaltete Geräte mit dem klbackup-Tool unter die Verwaltung eines anderen Administrationsservers:

1. Erstellen Sie auf dem bisherigen Gerät eine Backup-Kopie vom Zertifikat des Administrationsservers und von dessen privatem Schlüssel.

   Eine Backup-Kopie können Sie mit einer der folgenden Methoden erstellen:

   - Unter Verwendung des klbackup-Tools und dessen Benutzeroberfläche (nur für Administrationsserver unter Kaspersky Security Center Windows)

     Starten Sie das klbackup-Tool aus dem Installationsordner von Kaspersky Security Center und legen Sie anschließend mit der Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** ein Backup an.

   - Unter Verwendung der Eingabeaufforderung (für Administrationsserver ab Version 15.1 für Kaspersky Security Center Windows und Kaspersky Security Center Linux)

Führen Sie das klbackup-Tool mit dem Parameter `-cert_only` über die Befehlszeile aus, um eine Backup-Kopie des Zertifikats und des privaten Schlüssels des Administrationsservers anzulegen:

```
klbackup -path <Pfad zur Backup-Kopie des Administrationsserver-Zertifikats> -cert_only
```

2. Trennen Sie den Administrationsserver auf dem vorherigen Gerät vom Netzwerk.

3. Weisen Sie dem Gerät mit dem anderen Administrationsserver dieselbe Adresse zu.

   Dem neuen Administrationsserver können der NetBIOS-Name, der FQDN und die statische IP-Adresse zugewiesen werden. Dies hängt davon ab, welche Adresse für den Administrationsagenten im Installationspaket des Administrationsagenten angegeben wurde, als die Administrationsagenten verteilt wurden. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools klnagchk ermittelt werden).

4. Stellen Sie auf dem Gerät mit dem anderen Administrationsserver das Zertifikat des Administrationsservers und den privaten Schlüssel aus der Backup-Kopie wieder her.

   Eine Backup-Kopie können Sie mit einer der folgenden Methoden wiederherstellen:

   - Unter Verwendung des klbackup-Tools und dessen Benutzeroberfläche (nur für Administrationsserver unter Kaspersky Security Center Windows)

     Starten Sie das klbackup-Tool und stellen Sie anschließend das Backup mithilfe der Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** wieder her.

   - Unter Verwendung der Eingabeaufforderung (für Administrationsserver ab Version 15.1 für Kaspersky Security Center Windows und Kaspersky Security Center Linux)

     Führen Sie das klbackup-Tool mit dem Parameter `-cert_only` über die Befehlszeile aus, um eine Backup-Kopie des Zertifikats und des privaten Schlüssels des Administrationsservers wiederherzustellen:

     ```
     klbackup -path <Pfad zur Backup-Kopie des Administrationsserver-Zertifikats> -restore -cert_only
     ```

Die verwalteten Geräte werden unter die Verwaltung eines anderen Administrationsservers gestellt. Sie können zu diesem Administrationsserver wechseln. Stellen Sie aber sicher, dass die verwalteten Geräte im Netzwerk sichtbar sind und dass der Administrationsagent auf ihnen installiert ist und ausgeführt wird (in folgenden Spalten muss der Wert auf *Yes* stehen: **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt**).

Daten des Administrationsservers bei Verwendung von MySQL oder MariaDB sichern und wiederherstellen

Sie können ein Daten-Backup verwenden, um die Daten des Administrationsservers für Kaspersky Security Center Windows in die Verwaltung von Kaspersky Security Center Linux zu migrieren. Die Migration mittels Backups der Administrationsserver-Daten wird bei einer Migration auf Kaspersky Security Center Linux 15.2 oder höher nur für die unterstützten Versionen von Kaspersky Security Center Windows unterstützt.

Wenn Sie MySQL oder MariaDB als DBMS für Kaspersky Security Center Windows und für Kaspersky Security Center Linux verwenden, muss der Parameter `lower_case_table_names` für das aktuelle und das neue DBMS übereinstimmen. Andernfalls werden die Daten des Administrationsservers nicht korrekt migriert.

Prüfen Sie daher den Wert des Parameters `lower_case_table_names`, bevor Sie ein Backup der Daten des Administrationsservers für Kaspersky Security Center Windows anlegen. Wenn Sie diesen Parameter während der DBMS-Installation nicht angeben, wird der Standardwert des Parameters verwendet. Standardmäßig besitzt der Parameter `lower_case_table_names` unter Windows den Wert `1`.

Wenn Sie MySQL oder MariaDB für Kaspersky Security Center Linux installieren, setzen Sie den Wert des Parameters `lower_case_table_names` auf den Wert, wie er laut Anleitung von der MySQL-Website für den Parameter unter Windows vorgesehen ist. Wenn Sie diesen Parameter nicht angeben, wird der Standardwert des Parameters verwendet. Der Standardwert des Parameters `lower_case_table_names` ist für Linux-basierte Betriebssysteme und Windows verschieden.

Wenn Sie MySQL 8.0 installieren möchten, kann der Parameter `lower_case_table_names` möglicherweise nicht nach dieser Anleitung angegeben werden. In diesem Fall müssen Sie zuerst MySQL 5.7 installieren und den Parameter `lower_case_table_names` mithilfe der Anleitung angeben. Anschließend können Sie das installierte MySQL 5.7 auf MySQL 8.0 aktualisieren. Wenn der Parameter `lower_case_table_names` für das aktuelle und das neue DBMS nicht übereinstimmt, werden die Daten des Administrationsservers nicht korrekt wiederhergestellt.

Erstellen und Wiederherstellen eines Backups der Daten des Administrationsservers optimieren

Um durch Optimierung von Backup und der Wiederherstellung der Administrationsserver-Daten die Ausfallzeiten des Administrationsservers zu reduzieren, führen Sie einen der folgenden Schritte aus:

- Aktivieren Sie die Option **Dateisystem-Snapshot beim Anlegen eines Daten-Backups benutzen**.

  Weitere Informationen finden Sie im folgenden Artikel: Nutzung von Snapshots des Dateisystems zur Verkürzung der Dauer des Verschiebens ins Backup.

- Konfigurieren Sie die folgenden Flags:

  Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

  - `KLSRV_BKP_FILES` – Teilt die Datenbankdatei in mehrere kleinere Dateien von 2 bis 32 auf. Dies kann die Sicherung und Wiederherstellung beschleunigen, wenn die DBMS-Performance durch die CPU limitiert wird.

    Beispiel:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
    ```

  - `KLSRV_BKP_BACKUP_EXTRA_PARS` – Gibt die Parameter `COMPRESSION` und `MAXTRANSFERSIZE` an. Dies kann die Sicherung beschleunigen, wenn die DBMS-Performance durch den Input/Output limitiert wird.

    Beispiel:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
    MAXTRANSFERSIZE = 4194304"
    ```

  - `KLSRV_BKP_RESTORE_EXTRA_PARS` – Gibt den Parameter `MAXTRANSFERSIZE` an. Dies kann die Wiederherstellung beschleunigen, wenn die DBMS-Performance durch den Input/Output limitiert wird.

    Beispiel:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
    = 4194304"
    ```

- `KLSRV_BKP_ONLINE_DB_BACKUP` – verhindert Ausfallzeiten des Administrationsservers während der Backup-Erstellung. Nur für die folgenden DBMS verfügbar:

  - PostgreSQL und Postgres Pro

  - SQL Server mit dem vollständigen Wiederherstellungsmodell. Weitere Informationen finden Sie in der Dokumentation von SQL Server. Wenn Sie das Flag `KLSRV_BKP_ONLINE_DB_BACKUP` aktivieren, wechselt das SQL Server-DBMS automatisch auf das vollständige Wiederherstellungsmodell.

  Beispiel:

  ```
  klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
  ```

Administrationsserver auf anderes Gerät übertragen

Wenn Sie den Administrationsserver auf einem neuen Gerät verwenden müssen, können Sie ihn auf eine der folgenden Arten verschieben:

- Verschieben Sie den Administrationsserver und den Datenbankserver auf ein neues Gerät (der Datenbankserver kann auf dem neuen Gerät zusammen mit dem Administrationsserver oder auf einem anderen Gerät installiert werden).

- Belassen Sie den Datenbankserver auf dem bisherigen Gerät und verschieben Sie nur den Administrationsserver auf ein neues Gerät.

So übertragen Sie den Administrationsserver auf ein neues Gerät:

1. Erstellen Sie auf dem bisherigen Gerät ein Backup der Daten des Administrationsservers.

   Dazu können Sie entweder die Aufgabe zum Anlegen eines Daten-Backups über Verwaltungskonsole ausführen oder das Tool klbackup verwenden.

   > Wenn Sie derzeit SQL Server als DBMS für den Administrationsserver verwenden, können Sie die Daten von SQL Server zu MySQL oder MariaDB DBMS migrieren. Führen Sie dazu das Tool "klbackup" im interaktiven Modus aus, um ein Daten-Backup zu erstellen. Aktivieren Sie die Option **Auf MySQL/MariaDB-Format migrieren** im Fenster **Einstellungen für Backups** des Backup- und Wiederherstellungsassistenten. Kaspersky Security Center erstellt ein mit MySQL und MariaDB kompatibles Backup. Danach können Sie die Daten aus dem Backup in MySQL oder MariaDB wiederherstellen.

   > Sie können auch die Option **Auf Azure-Format migrieren** aktivieren, wenn Sie die Daten von SQL Server zu Azure SQL DBMS migrieren wollen.

2. Trennen Sie den Administrationsserver auf dem vorherigen Gerät vom Netzwerk.

3. Wählen Sie ein neues Gerät aus, auf dem der Administrationsserver installiert werden soll. Stellen Sie sicher, dass die Hardware und Software des ausgewählten Gerätes den Anforderungen des Administrationsservers, der Verwaltungskonsole und des Administrationsagenten entsprechen. Überprüfen Sie außerdem, ob die auf dem Administrationsserver verwendeten Ports verfügbar sind.

4. Weisen Sie dem neuen Gerät dieselbe Adresse zu.

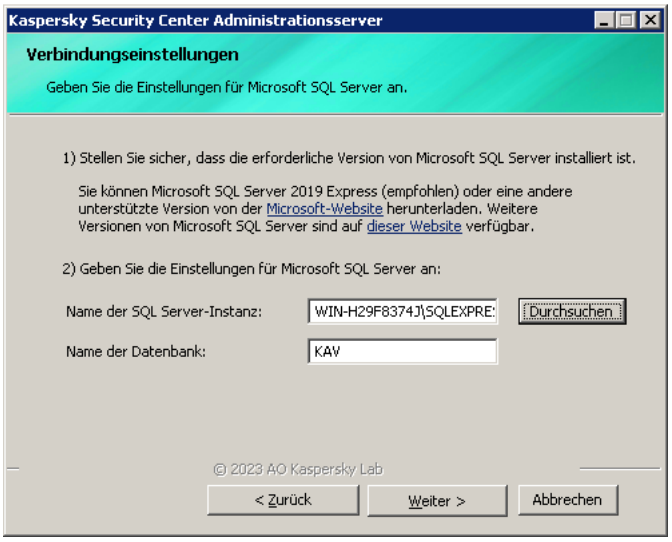
   Dem neuen Administrationsserver können der NetBIOS-Name, der FQDN und die statische IP-Adresse zugewiesen werden. Dies hängt davon ab, welche Adresse für den Administrationsagenten im Installationspaket des Administrationsagenten angegeben wurde, als die Administrationsagenten verteilt wurden. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools klnagchk ermittelt werden).

5. Installieren Sie das Datenbankverwaltungssystem (DBMS) bei Bedarf auf einem anderen Gerät, das vom Administrationsserver verwenden wird.

   Die Datenbank kann entweder zusammen mit dem Administrationsserver auf dem neuen Gerät oder auf einem anderen Gerät installiert werden. Stellen Sie sicher, dass dieses Gerät die Hard- und Softwarevoraussetzungen erfüllt. Berücksichtigen Sie bei der Auswahl eines DBMS die Anzahl der Geräte, die vom Administrationsserver verwaltetet werden.

6. Führen Sie auf dem neuen Gerät die Installation des Administrationsservers aus.

7. Konfigurieren Sie die Verbindungseinstellungen des Datenbankservers während der Installation des Administrationsservers.



Beispiel für das Fenster mit den Verbindungseinstellungen für Microsoft SQL Server

Führen Sie je nachdem, wo Sie den Datenbankserver platzieren müssen, einen der folgenden Schritte aus:

- **Belassen Sie den Datenbankserver auf dem vorherigen Gerät**

  1. Klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Name der SQL Server-Instanz** und wählen Sie in der angezeigten Liste den vorherigen Gerätenamen.

     Beachten Sie, dass das vorherige Gerät für die Verbindung mit dem neuen Administrationsserver verfügbar sein muss.

  2. Geben Sie den vorherigen Datenbanknamen im Feld **Name der Datenbank** ein.

- **Verschieben Sie den Datenbankserver auf das andere Gerät**

    1. Klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Name der SQL Server-Instanz** und wählen Sie anschließend den Gerätenamen, der in der Liste angezeigt wird.

    2. Geben Sie denen neuen Datenbankname im Feld **Name der Datenbank** ein.

        Beachten Sie, dass der neue Datenbankname mit dem Namen der Datenbank des vorherigen Geräts übereinstimmen muss. Die Namen der Datenbanken müssen identisch sein, damit Sie die Sicherung des Administrationsservers verwenden können. Der Standarddatenbankname ist *KAV*.

8. Stellen Sie nach Abschluss der Installation die Administrationsserver-Daten auf dem neuen Gerät mithilfe des Dienstprogramms klbackup wieder her.

    Wenn Sie als DBMS auf dem vorherigen und neuen Gerät SQL Server verwenden, beachten Sie, dass die auf dem neuen Gerät installierte Version von SQL Server mit der auf dem vorherigen Gerät installierten Version von SQL Server identisch oder höher sein muss. Andernfalls können Sie die Daten des Administrationsservers auf dem neuen Gerät nicht wiederherstellen.

9. Öffnen Sie die Verwaltungskonsole und verbinden Sie sich mit dem Administrationsserver.

10. Überprüfen Sie, ob alle verwalteten Geräte mit dem Administrationsserver verbunden sind.

11. Deinstallieren Sie den Administrationsserver und den Datenbankserver vom bisherigen Gerät.

Sie können auch die Kaspersky Security Center Web Console verwenden, um den Administrationsserver und einen Datenbankserver auf ein anderes Gerät zu verschieben.

Konflikte zwischen mehreren Administrationsservern vermeiden

Wenn Sie mehr als einen Administrationsserver in Ihrem Netzwerk verwenden, können diese dieselben Client-Geräte sehen. Dies kann Konflikten führen, wenn etwa ein Administrationsserver eine Anwendung installiert, die bereits von einem anderen Administrationsserver installiert wurde. Um zu verhindern, dass eine Anwendung auf einem Gerät installiert wird, das durch einen anderen Administrationsserver verwaltet wird, müssen Sie in den Eigenschaften der Aufgabe *Remote-Installation eines Programms* die Option **Nur auf Geräten installieren, die durch diesen Administrationsserver verwaltet werden** aktivieren.

Wenn Sie die Option **Nur auf Geräten installieren, die durch diesen Administrationsserver verwaltet werden** aktivieren und anschließend die Aufgabe *Remote-Installation eines Programms* ausführen, findet eine Prüfung statt, ob die Geräte von einem anderen Administrationsserver verwaltet werden. Für verwaltete Geräte, die durch einen anderen Administrationsserver verwaltet werden, wird der Wert des Attributs **Verwaltung erfolgt durch anderen Administrationsserver** auf `true` gesetzt. Die Aufgabe *Remote-Installation eines Programms* wird auf diese Geräte nicht angewendet.

Der Wert des Attributs **Verwaltung erfolgt durch anderen Administrationsserver** wird in der Spalte **Verwaltung erfolgt durch anderen Administrationsserver** der Liste der verwalteten Geräte und der Liste der nicht zugewiesenen Geräte angezeigt.

Sie können die Eigenschaft **Verwaltung erfolgt durch anderen Administrationsserver** auch als Kriterium für folgende Zwecke verwenden:

- Suche nach Geräten
- Geräteauswahlen
- Verschiebungsregeln für Geräte
- Regeln für die automatische Tag-Zuweisung

Um das Attribut Verwaltung erfolgt durch anderen Administrationsserver zurückzusetzen:

1. Wechseln Sie im Hauptmenü von Kaspersky Security Center Web Console zu **Gerätesuche und Bereitstellung → Nicht zugeordnete Geräte**.
2. Wählen Sie das gewünschte Gerät aus und klicken Sie anschließend auf die Schaltfläche **Entfernen Sie das Attribut "Verwaltung erfolgt durch anderen Administrationsserver"**.

Das Attribut **Verwaltung erfolgt durch anderen Administrationsserver** wird zurückgesetzt.

Administrationsgruppen verwalten

Der Abschnitt enthält Informationen über die Arbeit mit den Administrationsgruppen.

Sie können mit den Administrationsgruppen folgende Aktionen ausführen:

- eine beliebige Anzahl von untergeordneten Gruppen aller Hierarchieebenen zu einer Administrationsgruppe hinzufügen
- Geräte zu Administrationsgruppen hinzufügen
- Hierarchie der Administrationsgruppen durch Verschieben einzelner Geräte und ganzer Gruppen in andere Gruppen ändern
- Untergruppen und Geräte aus Administrationsgruppen löschen
- Dem Verzeichnis der Administrationsgruppen sekundäre und virtuelle Administrationsserver hinzufügen
- Geräte aus Administrationsgruppen eines Administrationsservers in die Gruppen eines anderen Servers verschieben
- Festlegen, welche Kaspersky-Anwendungen automatisch auf den Geräten installiert werden sollen, die in eine Gruppe aufgenommen werden

Sie können diese Aktionen nur dann durchführen, wenn Sie die Berechtigung **Ändern** im Bereich **Verwaltung von Administrationsgruppen** für die Administrationsgruppe (oder für den Administrationsserver, zu dem diese Gruppen gehören) haben, die Sie ändern möchten.

Administrationsgruppen anlegen

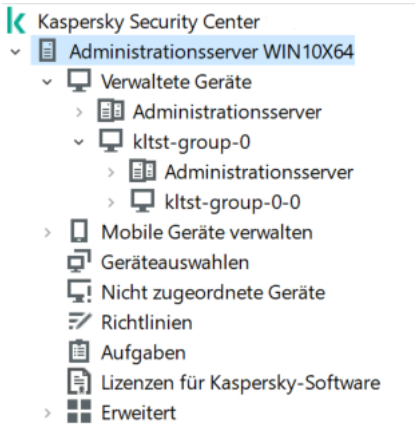
Die Hierarchie der Administrationsgruppen wird im Programmhauptfenster von Kaspersky Security Center im Ordner **Verwaltete Geräte** erstellt. Die Administrationsgruppen werden als Ordner in der Konsolenstruktur angezeigt (s. Abb. unten).

Sofort nach der Installation von Kaspersky Security Center enthält der Ordner **Verwaltete Geräte** nur den leeren Ordner **Administrationsserver**.

Ob der Ordner **Administrationsserver** in der Konsolenstruktur vorhanden ist, wird durch die Einstellungen der Benutzeroberfläche definiert. Um die Anzeige dieses Ordners zu aktivieren, wechseln Sie in das Menü **Ansicht** → **Benutzeroberfläche anpassen**, und aktivieren Sie im Fenster **Benutzeroberfläche anpassen** das Kontrollkästchen **Sekundäre Administrationsserver anzeigen**.

Wenn Sie eine Hierarchie der Administrationsgruppen erstellen, können Sie Geräte und virtuelle Maschinen zum Ordner **Verwaltete Geräte** hinzufügen und untergeordnete Gruppen hinzufügen. Im Ordner **Administrationsserver** können Sie sekundäre und virtuelle Administrationsserver hinzufügen.

Jede erstellte Gruppe enthält zunächst (auch wie der Ordner **Verwaltete Geräte**) den leeren Ordner **Administrationsserver**, der für die Arbeit mit den sekundären und virtuellen Administrationsservern der entsprechenden Gruppe vorgesehen ist. Informationen zu Richtlinien und Aufgaben für diese Gruppe sowie Informationen über die Geräte, die zu dieser Gruppe gehören, werden auf den Registerkarten mit den entsprechenden Namen im Arbeitsbereich dieser Gruppe angezeigt.



Hierarchie der Administrationsgruppen erstellen

Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte**.

2. Wenn Sie eine untergeordnete Gruppe für eine vorhandene Administrationsgruppe erstellen möchten, wählen Sie im Ordner **Verwaltete Geräte** den Unterordner, welcher der Gruppe entspricht, zu der die neue Administrationsgruppe gehören soll.

   Wenn Sie eine neue Administrationsgruppe der obersten Hierarchieebene erstellen, können Sie diesen Schritt überspringen.

3. Starten Sie den Vorgang zum Erstellen einer Administrationsgruppe auf eine der folgenden Arten:

   - Mit dem Kontextmenübefehl **New → Gruppe**
   - Mit der Schaltfläche **Neue Gruppe**, die sich im Arbeitsbereich des Programmhauptfensters auf der Registerkarte **Geräte** befindet

4. Geben Sie im folgenden Fenster **Gruppenname** den Namen der Gruppe ein, und klicken Sie auf **OK**.

   Daraufhin wird in der Konsolenstruktur ein neuer Ordner der Administrationsgruppe mit dem angegebenen Namen angezeigt.

Das Programm ermöglicht, die Gruppenstruktur der Administrationsgruppen auf der Grundlage der Struktur von Active Directory oder der Struktur des Domänennetzwerks zu erstellen. Darüber hinaus können Sie die Gruppenstruktur auch aus einer Textdatei erstellen.

Um die Struktur der Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
2. Klicken Sie im Kontextmenü des Ordners **Verwaltete Geräte** auf **Alle Aufgaben → Neue Gruppenstruktur**.

   Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Anweisungen des Assistenten.

Administrationsgruppen verschieben

Sie können untergeordnete Administrationsgruppen innerhalb der Hierarchie der Gruppen verschieben.

Die Administrationsgruppe wird zusammen mit allen Untergruppen, sekundären Administrationsservern, Geräten sowie Gruppenrichtlinien und -aufgaben verschoben. Das System wendet sämtliche Einstellungen auf die Gruppe an, die ihrer neuen Position in der Hierarchie der Administrationsgruppen entsprechen.

Der Gruppenname muss innerhalb einer Hierarchieebene einmalig sein. Wenn im Ordner, in den Sie die Administrationsgruppe verschieben, eine Gruppe mit dem gleichen Namen bereits vorhanden ist, ändern Sie den Namen der Gruppe vor dem Verschieben. Wenn Sie den Namen der zu verschiebenden Gruppe zuvor nicht geändert haben, wird dem Namen der Gruppe beim Verschieben die Endung **_<laufende Nummer>** (z.B. **(1)**, **(2)**) hinzugefügt.

Sie können den Namen der Gruppe **Verwaltete Geräte** nicht ändern, da der Ordner ein integraler Bestandteil der Verwaltungskonsole ist.

Um eine Gruppe in einen anderen Ordner der Konsolenstruktur zu verschieben, gehen Sie wie folgt vor:

1. Wählen Sie die zu verschiebende Gruppe in der Konsolenstruktur aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verschieben Sie die Gruppe mit dem Kontextmenü:
     1. Klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie **Ausschneiden** aus.
     2. Klicken Sie danach mit der rechten Maustaste auf die Administrationsgruppe, in welche die gewählte Gruppe verschoben werden soll, und wählen Sie **Einfügen** aus.
   - Verwenden Sie das Programmhauptmenü, um die Gruppe zu verschieben:
     a. Wählen Sie im Hauptmenü **Aktion** → **Ausschneiden** aus.
     b. Wählen Sie danach in der Konsolenstruktur die Administrationsgruppe aus, in welche die gewählte Gruppe verschoben werden soll.
     c. Wählen Sie im Hauptmenü **Aktion** → **Einfügen** aus.
   - Verschieben Sie die Gruppe in eine andere Gruppe mit der Maus.

Deleting administration groups

Sie können eine Administrationsgruppe löschen, wenn sie keine sekundären Administrationsserver, verschachtelten Gruppen und Client-Geräte enthält und wenn für sie keine Gruppenaufgaben oder Richtlinien erstellt wurden.

Bevor eine Administrationsgruppe gelöscht wird, ist es erforderlich, sekundäre Administrationsserver, Gruppen und Client-Geräte daraus zu löschen.

Um eine Gruppe zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie **Entfernen** aus.
   - Klicken Sie mit der rechten Maustaste auf das Hauptmenü des Programms und wählen **Aktion** → **Entfernen** aus.
   - Drücken Sie die Taste **`Entf`**.

Administrationsgruppenstruktur automatisch anlegen

Kaspersky Security Center ermöglicht es, automatisch mithilfe des Assistenten für das Erstellen einer Gruppenhierarchie eine Struktur der Administrationsgruppen zu erstellen.

Der Assistent erstellt eine Struktur der Administrationsgruppen auf Grundlage folgender Daten:

- Domänenstruktur und Struktur der Arbeitsgruppen des Windows-Netzwerks.
- Gruppenstruktur des Active Directory.
- Inhalt einer Textdatei, die vom Administrator manuell erstellt wurde.

Beim Erstellen einer Textdatei sind folgende Regeln einzuhalten:

- Der Name jeder neuen Gruppe beginnt in einer neuen Zeile. Das Trennungszeichen ist der Zeilenumbruch. Leere Zeilen werden ignoriert.

  Beispiel:
  Büro 1
  Büro 2
  Büro 3
  In der Zielgruppe werden drei Gruppen der ersten Hierarchieebene angelegt.

- Der Name der eingebetteten Gruppe muss hinter dem Schrägstrich (/) eingegeben werden.

  Beispiel:
  Büro 1/Untereinheit 1/Abteilung 1/Gruppe 1
  In der Zielgruppe werden vier zueinander eingebettete Untergruppen angelegt.

- Um mehrere eingebettete Gruppen einer Hierarchieebene anzulegen, muss ein "vollständiger Pfad zur Gruppe" eingegeben werden.

  Beispiel:
  Büro 1/Untereinheit 1/Abteilung 1
  Büro 1/Untereinheit 2/Abteilung 1
  Büro 1/Untereinheit 3/Abteilung 1
  Büro 1/Untereinheit 4/Abteilung 1
  In der Zielgruppe wird eine Gruppe der ersten Hierarchieebene "Büro 1" angelegt, zu der vier eingebettete Gruppen einer Hierarchieebene "Untereinheit 1", "Untereinheit 2", "Untereinheit 3", "Untereinheit 4" gehören. Zu jeder Gruppe gehört eine Gruppe "Abteilung 1".

Das Erstellen der Administrationsgruppenstruktur mit dem Assistenten verletzt die Integrität des Netzwerks nicht: Neue Gruppen werden hinzugefügt, ersetzen aber nicht die vorhandenen Gruppen. Ein Client-Gerät kann zu einer Administrationsgruppe nicht erneut hinzugefügt werden, weil das Gerät beim Verschieben in die Administrationsgruppe aus der Gruppe **Nicht zugeordnete Geräte** gelöscht wird.

Wenn beim Anlegen der Gruppenstruktur ein Gerät aus einem beliebigen Grund in der Gruppe **Nicht zugeordnete Geräte** nicht aufgenommen wird (ausgeschaltet, vom Netzwerk getrennt), dann wird es zur Administrationsgruppe nicht automatisch hinzugefügt. Sie können Geräte zu Administrationsgruppen manuell nach Abschluss des Assistenten hinzufügen.

Um das automatische Erstellen einer Administrationsgruppe zu starten, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
2. Klicken Sie im Kontextmenü des Ordners **Verwaltete Geräte** auf **Alle Aufgaben → Neue Gruppenstruktur**.

   Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Anweisungen des Assistenten.

Programme automatisch auf Geräten einer Administrationsgruppe installieren

Sie können angeben, welche Installationspakete für die automatische Remote-Installation von Kaspersky-Anwendungen auf Client-Geräten in einer Administrationsgruppe verwendet werden sollen.

Um die automatische Installation von Anwendungen auf den Geräten in einer Administrationsgruppe zu konfigurieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die gewünschte Administrationsgruppe aus.
2. Öffnen Sie das Eigenschaftenfenster dieser Administrationsgruppe.
3. Wählen Sie im Bereich **Abschnitte** die Option **Automatische Installation** aus und wählen Sie anschließend im Arbeitsbereich die Installationspakete der Anwendungen aus, die auf den Geräten installiert werden sollen.
4. Klicken Sie auf die Schaltfläche **OK**.

Gruppenaufgaben werden erstellt. Diese Aufgaben werden auf den Client-Geräten gestartet, direkt nachdem diese zu der Administrationsgruppe hinzugefügt wurden.

Wenn für die automatische Installation mehrere Installationspakete einer Anwendung angegeben werden, wird die Installationsaufgabe nur für die neueste Version der Anwendung erstellt.

Verwaltung von Client-Geräten

Der Abschnitt enthält Informationen über die Arbeit mit den Client-Geräten.

Client-Geräte mit dem Administrationsserver verbinden

Eine Verbindung zwischen einem Client-Gerät und dem Administrationsserver wird durch den auf dem Client-Gerät installierten Administrationsagenten hergestellt.

Beim Herstellen einer Verbindung zwischen dem Client-Gerät und dem Administrationsserver werden folgende Vorgänge ausgeführt:

- Automatische Synchronisierung der Daten:
  - Synchronisierung der Liste der Programme, die auf dem Client-Gerät installiert sind
  - Synchronisierung von Richtlinien, Programmeinstellungen, Aufgaben und Aufgabeneinstellungen
- Empfang von aktuellen Daten über den Status der Programme, Aufgabenausführung und Statistikdaten der Programme durch den Administrationsserver
- Senden der Daten an den Administrationsserver über die Ereignisse, die verarbeitet werden sollen

Die automatische Datensynchronisierung erfolgt regelmäßig in Abhängigkeit von den Einstellungen des Administrationsagenten (beispielsweise alle 15 Minuten). Sie können das Verbindungsintervall manuell angeben.

Die Ereignisdaten werden sofort nach Eintritt des Ereignisses an den Administrationsserver gesendet.

Wenn sich der Administrationsserver an einem Remotestandort (außerhalb des Firmennetzwerks) befindet, werden die Client-Geräte via Internet mit diesem verbunden.

Zum Herstellen einer Internetverbindung zwischen Geräten und dem Administrationsserver müssen folgende Bedingungen erfüllt sein:

- Der Remote-Administrationsserver benötigt eine externe IP-Adresse, wobei der Eingangsport 13000 (für Verbindungen von Administrationsagenten) geöffnet sein muss. Es wird empfohlen, zusätzlich den UDP-Port 13000 (für die Annahme von Benachrichtigungen über die Deaktivierung von Geräten) zu öffnen.
- Auf den Geräten müssen Administrationsagenten installiert sein.
- Bei der Installation des Administrationsagenten auf den Geräten muss die IP-Adresse des Remote-Administrationsservers angegeben werden. Wenn für die Installation ein Installationspaket verwendet wird, muss die externe IP-Adresse manuell in den Eigenschaften des Installationspaketes im Abschnitt **Einstellungen** eingegeben werden.
- Um Programme und Aufgaben eines Geräts mit dem Administrationsserver verwalten zu können, aktivieren Sie im Eigenschaftenfenster des Geräts im Abschnitt **Allgemein** das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**. Nachdem Sie das Kontrollkästchen aktiviert haben, warten Sie auf die Synchronisierung des Administrationsservers mit dem Remote-Gerät. Eine ununterbrochene Verbindung mit dem Administrationsserver wird für maximal 300 Client-Geräte zugleich unterstützt.

Um die Ausführung der Aufgaben zu beschleunigen, die vom Remote-Administrationsserver eingehen, können Sie auf dem Gerät den Port 15000 öffnen. In diesem Fall sendet der Administrationsserver zum Starten der Aufgabe über den Port 15000 ein spezielles Paket an den Administrationsagenten, ohne auf den Abschluss der Synchronisierung mit dem Gerät zu warten.

Kaspersky Security Center erlaubt, die Verbindung zwischen einem Client-Gerät und dem Administrationsserver so einzustellen, dass die Verbindung nach Abschluss eines Vorgangs nicht getrennt wird. Eine ununterbrochene Verbindung wird dann gebraucht, wenn der Programmstatus ständig kontrolliert werden soll und der Administrationsserver keine Verbindung zum Client-Gerät herstellen kann (Die Verbindung ist beispielsweise durch eine Firewall geschützt, Ports dürfen auf dem Client-Gerät nicht geöffnet werden, IP-Adresse des Client-Geräts ist nicht bekannt usw.). Eine ununterbrochene Verbindung zwischen einem Client-Gerät und dem Administrationsserver können Sie im Eigenschaftenfenster des Client-Geräts im Abschnitt **Allgemein** herstellen.

Es wird empfohlen, mit den wichtigsten Geräten eine ununterbrochene Verbindung herzustellen. Die Gesamtzahl der Verbindungen, die vom Administrationsserver gleichzeitig unterstützt werden, ist auf 300 beschränkt.

Bei einer manuellen Synchronisierung wird eine Hilfsmethode für das Herstellen einer Verbindung verwendet. Bei dieser Methode wird die Verbindung durch den Administrationsserver initiiert. Öffnen Sie vor dem Verbindungsaufbau den entsprechenden UDP-Port auf dem Client-Gerät. Der Administrationsserver schickt die Anfrage zum Verbindungsaufbau an den UDP-Port des Client-Geräts. Daraufhin wird das Zertifikat des Administrationsservers überprüft. Stimmt das Zertifikat des Administrationsservers mit dessen Kopie auf dem Client-Gerät überein, wird die Verbindung aufgebaut.

Der manuelle Start des Synchronisierungsvorgangs wird verwendet, wenn Sie aktuelle Informationen über den Status der Programme, Aufgabenausführung und Statistikdaten über die Programme empfangen möchten.

Client-Gerät manuell mit Administrationsserver verbinden. Tool klmover

Wenn es erforderlich ist, ein Client-Gerät mit dem Administrationsserver manuell zu verbinden, können Sie das Tool klmover auf dem Client-Gerät verwenden.

Bei der Installation des Administrationsagenten auf dem Client-Gerät wird das Tool automatisch in den Installationsordner des Administrationsagenten kopiert.

Um ein Client-Gerät zum Administrationsserver mit dem Tool klmover manuell zu verbinden,

starten Sie auf dem Gerät das Tool klmover über die Befehlszeile.

Beim Starten über die Befehlszeile führt das Tool klmover je nach Parameter die folgenden Aktionen aus:

- Verbinden des Administrationsagenten mit dem Administrationsserver mit den angegebenen Einstellungen.
- Eintragen der Ergebnisse dieses Vorgangs in die Log-Datei oder Darstellung der Ergebnisse auf dem Bildschirm.

Sie können das Tool "klmover" nicht für Client-Geräte verwenden, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind. Für solche Geräte müssen Sie entweder den Administrationsagenten neu konfigurieren oder den Administrationsagenten neu installieren und das Verbindungs-Gateway angeben.

Die Befehlszeilensyntax des Tools lautet:

```
klmover [-logfile <Dateiname>] [-address <Serveradresse>] [-pn <Portnummer>] [-ps
<SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatsdatei>] [-silent] [-dupfix] [-
virtserv] [-cloningmode]
```

Zum Ausführen des Tools sind Administratorrechte erforderlich.

Die Schlüssel weisen folgende Bedeutung auf:

- `-logfile <Dateiname>` – Ergebnisse der Tool-Ausführung in Log-Datei schreiben.

  Standardmäßig werden die Informationen im Standardausgabe-Stream (stdout) gespeichert. Wenn der Schlüssel nicht verwendet wird, werden die Ergebnisse und Fehlermeldungen auf dem Bildschirm angezeigt.

- `-address <Serveradresse>` – Adresse des Administrationsservers, zu dem eine Verbindung hergestellt werden soll.

  Es kann die IP-Adresse, der NetBIOS-Name oder der DNS-Name des Geräts angegeben werden.

- `-pn <Portnummer>` – Nummer des Ports, über den eine ungesicherte Verbindung zum Administrationsserver hergestellt wird.

  Standardmäßig wird Portnummer 14000 verwendet.

- `-ps <SSL-Portnummer>` – Nummer des SSL-Ports, über den eine gesicherte Verbindung zum Administrationsserver mit dem SSL-Protokoll hergestellt wird.

  Standardmäßig wird Portnummer 13000 verwendet.

- `-nossl` – Ungesicherte Verbindung zum Administrationsserver verwenden.

  Wenn kein Schlüssel verwendet wird, erfolgt die Verbindung des Administrationsagenten mit dem Administrationsserver über das SSL-Protokoll.

- `-cert <Pfad zur Zertifikatsdatei>` – Angegebene Zertifikatsdatei für Authentifizierung am Administrationsserver verwenden.

  Wenn kein Schlüssel angegeben wird, empfängt der Administrationsagent das Zertifikat beim ersten Verbinden mit dem Administrationsserver.

- `-silent` – Tool im Silent-Modus starten.

  Der Einsatz dieses Parameters kann sehr nützlich sein, wenn das Tool beispielsweise über ein Anmeldeskript bei der Anmeldung eines Benutzers aufgerufen wird.

- `-dupfix` – Dieser Schlüssel kommt zum Einsatz, wenn der Administrationsagent nicht auf die konventionelle Weise mit den Dateien im Programmpaket, sondern beispielsweise über die Wiederherstellung eines ISO-Disk-Images installiert wurde.

- `-virtserv` – Name des virtuellen Administrationsservers.

- `-cloningmode` – Modus des Administrationsagenten zum Klonen von Laufwerken.

  Verwenden Sie einen der folgenden Parameter, um den Modus zum Klonen von Laufwerken zu konfigurieren:

  - `-cloningmode` – Status des Modus zum Klonen von Laufwerken abfragen.
  - `-cloningmode 1` – Modus zum Klonen von Laufwerken aktivieren.
  - `-cloningmode 0` – Modus zum Klonen von Laufwerken deaktivieren.

- `-nauninstpwd <Kennwort>` – Parameter zum Angeben des Deinstallationskennworts des Administrationsagenten.

  Der Parameter ist nicht obligatorisch.

Um beispielsweise den Administrationsagenten mit dem Administrationsserver zu verbinden, führen Sie den folgenden Befehl aus:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Verbindung des Client-Geräts mit dem Administrationsserver tunneln

Kaspersky Security Center erlaubt das Tunneln der TCP-Verbindungen von der Verwaltungskonsole über den Administrationsserver und weiter über den Administrationsagenten zum angegebene Port auf dem verwalteten Gerät. Das Tunneln wird für den Fall, dass eine direkte Verbindung des Geräts mit der Verwaltungskonsole unmöglich ist, für die Verbindung des Client-Programms, welches sich auf dem Gerät mit der installierten Verwaltungskonsole befindet, zum TCP-Port des verwalteten Gerät verwendet.

Insbesondere wird das Tunneln für die Remotedesktopverbindung verwendet: sowohl für die Verbindung mit einer bestehenden Sitzung, als auch für das Erstellen einer neuen Remote-Sitzung.

Ferner kann das Tunneln mithilfe von externen Tools verwendet werden. Insbesondere kann der Administrator so das Tool putty, den VNC-Client und weitere Tools starten.

Es ist erforderlich, die Verbindung eines Remote-Client-Geräts mit dem Administrationsserver zu tunneln, wenn der Port für die Verbindung mit dem Administrationsserver auf dem Gerät nicht verfügbar ist. Der Port auf dem Gerät kann in folgenden Fällen nicht verfügbar sein:

- Das Remote-Gerät ist mit einem lokalen Netzwerk verbunden, in dem das NAT-Verfahren verwendet wird.
- Das Remote-Gerät gehört zum lokalen Netzwerk des Administrationsservers, sein Port wird jedoch von der Firewall geschlossen.

Um die Verbindung zwischen einem Client-Gerät und dem Administrationsserver zu tunneln, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner der Gruppe, zu welcher das Client-Gerät gehört.
2. Wählen Sie auf der Registerkarte **Geräte** ein Gerät aus.
3. Wählen Sie im Kontextmenü des Geräts den Punkt **Alle Aufgaben → Verbindung tunneln**.
4. Erstellen Sie im folgenden Fenster **Verbindung tunneln** einen Tunnel.

Remotedesktopverbindung mit dem Client-Gerät herstellen

Der Administrator kann Remotezugriff auf den Desktop des Client-Geräts mithilfe des Administrationsagenten bekommen, der auf dem Client-Gerät installiert wurde.

Die Remoteverbindung mit dem Client-Gerät mithilfe des Administrationsagenten ist sogar dann möglich, wenn die TCP- und UDP-Ports des Client-Geräts geschlossen sind. Nach der Verbindung mit dem Gerät bekommt der Administrator vollständigen Zugriff auf die Informationen dieses Geräts und kann die auf diesem Gerät installierten Programme verwalten.

In diesem Abschnitt wird beschrieben, wie Sie über den Administrationsagent eine Verbindung zu einem Windows-Client-Gerät und einem macOS-Client-Gerät herstellen.

Eine Verbindung mit Windows-Client-Geräten herstellen

Die Remoteverbindung mit dem Windows-basierten Client-Gerät kann auf zwei Arten hergestellt werden:

- Mithilfe der Standard-Komponente von Microsoft Windows "Remotedesktopverbindung".

  Die Remotedesktopverbindung erfolgt mithilfe des Windows-Standardtools mstsc.exe gemäß den Einstellungen des Dienstprogramms.

- Mithilfe der Windows Desktopfreigabe.

Herstellen einer Verbindung mit dem Windows-basierten Client-Gerät mittels Remotedesktopverbindung

Die Verbindung zu einer bestehenden Sitzung des Remotedesktops des Benutzers wird ohne Benachrichtigung des Benutzers hergestellt. Nachdem sich der Administrator mit der Sitzung verbunden hat, wird der Benutzer des Client-Geräts ohne vorherige Benachrichtigung von der Sitzung abgemeldet.

Gehen Sie wie folgt vor, um eine Remotedesktopverbindung mit dem Client-Gerät mithilfe der Komponente "Remotedesktopverbindung" herzustellen:

1. Wählen Sie in der Verwaltungskonsole ein Client-Gerät aus, auf das zugegriffen werden soll.
2. Wählen Sie im Kontextmenü des Geräts den Punkt **Alle Aufgaben → Mit Gerät verbinden → Neue RDP-Sitzung**.

   Daraufhin wird das Windows-Standardtool mstsc.exe zum Herstellen einer Remotedesktopverbindung gestartet.
3. Folgen Sie den Anweisungen in den Fenstern des Tools.

Nach der Verbindung mit dem Client-Gerät ist der Desktop des Client-Geräts im Microsoft Windows-Fenster für Remoteverbindung verfügbar.

Eine Verbindung mit einem Windows-basierten Client-Gerät unter Verwendung der Windows Desktopfreigabe herstellen

Bei der Verbindung mit einer vorhandenen Remotedesktop-Sitzung empfängt der Benutzer der Sitzung auf dem Gerät eine Anfrage zum Herstellen der Verbindung vom Administrator. Die Informationen über die Aktivitäten auf dem Remote-Gerät und deren Ergebnisse werden in den Kaspersky Security Center-Berichten nicht gespeichert.

Der Administrator kann eine Verbindung mit der vorhandenen Sitzung auf dem Client-Gerät herstellen, ohne dass der Benutzer dieser Sitzung getrennt wird. In diesem Fall haben der Administrator und der Benutzer der Sitzung auf dem Gerät einen gemeinsamen Zugriff auf den Desktop.

Der Administrator kann ein Audit der Aktionen auf dem Remote-Client-Gerät konfigurieren. Während des Audits werden Informationen über die Dateien auf dem Client-Gerät gesammelt, die vom Administrator geöffnet bzw. geändert werden.

Um sich mittels Windows Desktopfreigabe mit dem Desktop eines Client-Geräts zu verbinden, müssen die folgenden Voraussetzungen erfüllt sein:

- Auf dem Administrator-Arbeitsplatz ist Microsoft Windows Vista oder höher installiert. Für die Herstellung einer Verbindung mithilfe der Windows Desktopfreigabe gibt es keine Einschränkungen hinsichtlich des Betriebssystemtyps des Geräts, auf dem der Administrationsserver installiert ist.

  Um zu prüfen, ob die Funktion für die Windows Desktopfreigabe in Ihrer Windows-Edition enthalten ist, stellen Sie sicher, dass der Schlüssel "CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F}" in der Windows-Registry enthalten ist.
- Microsoft Windows Vista oder höher ist auf dem Client-Gerät installiert.
- Kaspersky Security Center nutzt eine Lizenz für Schwachstellen- und Patch-Management.

Um eine Verbindung mit dem Client-Gerät-Desktop über Windows Desktopfreigabe herzustellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsole ein Client-Gerät aus, auf das zugegriffen werden soll.
2. Wählen Sie im Kontextmenü des Geräts den Punkt **Alle Aufgaben → Mit Gerät verbinden → Windows Desktopfreigabe**.

3. Wählen Sie im folgenden Fenster **Desktopsitzung auswählen** die Sitzung auf dem Client-Gerät, zu der eine Verbindung hergestellt werden soll.

   Bei einer erfolgreichen Verbindung mit dem Client-Gerät wird sein Desktop im Fenster **Kaspersky Remote Desktop Session Viewer** verfügbar.

4. Um die Interaktion mit dem Gerät zu beginnen, wählen Sie im Hauptmenü des Fensters **Kaspersky Remote Desktop Session Viewer** den Punkt **Aktionen → Interaktiver Modus** aus.

Das Tool **Kaspersky Remote Desktop Session Viewer** erfordert eine kommerzielle Lizenz.

Eine Verbindung mit macOS-Client-Geräten herstellen

Der Administrator kann das Virtual Network Computing System (VNC) verwenden, um eine Verbindung zu macOS-Geräten herzustellen.

Die Verbindung zu einem Remote-Desktop wird über einen VNC-Client hergestellt, der auf dem Gerät des Administrationsservers installiert ist. Der VNC-Client schaltet die Tastatur- und Maussteuerung vom Client-Gerät auf den Administrator um.

Wenn der Administrator eine Verbindung zum Remote-Desktop herstellt, erhält der Benutzer keine Benachrichtigungen oder Verbindungsanforderungen vom Administrator. Der Administrator verbindet sich mit einer vorhandenen Sitzung auf dem Client-Gerät, ohne dass der Benutzer dieser Sitzung getrennt wird.

Um sich mittels VNC-Client mit dem Desktop eines macOS-basierten Client-Geräts zu verbinden, müssen die folgenden Voraussetzungen erfüllt sein:

- Der VNC-Client ist auf dem Gerät des Administrationsservers installiert.
- Auf dem Client-Gerät sind Remote-Anmeldung und Remote-Verwaltung erlaubt.
- Der Benutzer hat dem Administrator den Zugriff auf das Client-Gerät in den **Teilen**-Einstellungen des macOS-Betriebssystems gewährt.

So verbinden Sie sich mit einem Client-Gerät mittels Virtual Network Computing System:

1. Wählen Sie in der Verwaltungskonsole ein Client-Gerät aus, auf das zugegriffen werden soll.
2. Wählen Sie im Kontextmenü des Geräts den Punkt **Alle Aufgaben → Verbindung tunneln**.
3. Führen Sie im geöffneten Fenster **Verbindung tunneln** das Folgende aus:

   a. Geben Sie im Abschnitt **1. Netzwerk-Port** die Nummer des Netzwerkports des Geräts an, mit dem Sie sich verbinden wollen.

      Standardmäßig ist die Portnummer 5900 festgelegt.

   b. Klicken Sie im Abschnitt **2. Tunnelung** auf die Schaltfläche **Tunnel herstellen**.

   c. Klicken Sie im Abschnitt **3. Netzwerk-Attribute** auf die Schaltfläche **Kopieren**.

4. Öffnen Sie den VNC-Client und fügen Sie die kopierten Netzwerkattribute in das Textfeld ein. Drücken Sie **`Bestätigen`**.

5. Zeigen Sie sich im nächsten Fenster die Informationen zum Zertifikat an. Wenn Sie der Verwendung des Zertifikats zustimmen, klicken Sie auf die Schaltfläche **Ja**.

6. Geben Sie im Fenster **Authentifizierung** die Anmeldeinformationen des Client-Geräts an und klicken Sie anschließend auf **OK**.

Verbindung mit den Client-Geräten über die Windows Desktopfreigabe herstellen

Um eine Verbindung mit einem Gerät über Windows Desktopfreigabe herzustellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur auf der Registerkarte **Geräte** den Ordner **Verwaltete Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der Geräte angezeigt.

2. Klicken Sie mit der rechten Maustaste auf das Client-Gerät, mit dem Sie eine Verbindung herstellen möchten, und wählen Sie im Kontextmenü **Mit Gerät verbinden → Windows Desktopfreigabe** aus.

   Das Fenster **Desktopsitzung auswählen** wird geöffnet.

3. Wählen Sie im Fenster **Desktopsitzung auswählen** eine Desktopsitzung aus, die zum Herstellen einer Verbindung mit dem Gerät verwendet werden soll.

4. Klicken Sie auf die Schaltfläche **OK**.

Es wird eine Verbindung mit dem Gerät hergestellt.

Einstellungen für den Neustart des Client-Geräts

Während der Ausführung, Installation oder Deinstallation von Kaspersky Security Center kann es erforderlich sein, dass ein Neustart des Client-Geräts durchgeführt wird. Sie können die Einstellungen für den Neustart nur für Geräte unter Windows festlegen.

Um die Einstellungen für den Neustart des Client-Geräts anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für welche der Neustart angepasst werden soll.

2. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien** aus.

3. Wählen Sie im Arbeitsbereich eine Richtlinie des Kaspersky Security Center Administrationsagenten aus der Richtlinienliste aus, und wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften**.

4. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Verwaltung des Neustarts** aus.

5. Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn ein Neustart des Geräts erforderlich ist.

   - Wählen Sie **Betriebssystem nicht neu starten** aus, um einen automatischen Neustart zu unterbinden.
   - Wählen Sie **Betriebssystem bei Bedarf automatisch neu starten** aus, um den automatischen Neustart zu erlauben.
   - Wählen Sie **Benutzer fragen**, wenn Sie die Zustimmung des Benutzers zum Neustart aktivieren möchten.

Sie können die Häufigkeit der Abfrage eines Neustarts angeben, einen erzwungenen Neustart und ein erzwungenes Schließen von Apps in gesperrten Sitzungen auf dem Gerät aktivieren, indem Sie die entsprechenden Kontrollkästchen in Zeiteinstellungen in Drehfeldern aktivieren.

6. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Eigenschaftenfenster der Richtlinie zu schließen.

Als Ergebnis des Neustarts wird das Betriebssystem auf dem Gerät konfiguriert.

Überwachung der Aktionen auf einem Remote-Client-Gerät

Die Anwendung ermöglicht die Durchführung eines Audits der Aktionen des Administrators auf einem Remote-Client-Gerät unter Windows. Während des Audits werden Informationen über die Dateien auf dem Gerät gesammelt, die vom Administrator geöffnet bzw. geändert werden. Das Audit des Administrators ist unter folgenden Bedingungen verfügbar:

- Die Lizenz für das Schwachstellen- und Patch-Management wird verwendet.
- Der Administrator verfügt über die Berechtigung zum Start der Desktopfreigabe auf dem Remote-Gerät.

Um das Audit auf dem Remote-Client-Gerät zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die das Audit der Aktionen des Administrators konfiguriert werden soll.
2. Wählen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie des Kaspersky Security Center Administrationsagenten, und wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften**.
4. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Windows Desktopfreigabe** aus.
5. Aktivieren Sie das Kontrollkästchen **Audit aktivieren**.
6. Fügen Sie in den Listen **Masken der Dateien, die bei Lesezugriff überwacht werden sollen** und **Masken der Dateien, die auf Änderung überwacht werden sollen** die Masken hinzu, mit denen die Anwendung während des Audits Aktionen überwachen soll.

   Standardmäßig werden Aktionen mit Dateien mit den Erweiterungen .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt, .pdf geloggt.

7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Eigenschaftenfenster der Richtlinie zu schließen.

Als Ergebnis wird das Audit der Aktionen des Administrators auf dem Remote-Gerät des Benutzers bei Verwendung der Desktopfreigabe konfiguriert.

Einträge über die Aktionen des Administrators auf dem Remote-Gerät werden wie folgt gespeichert:

- Im Ereignisprotokoll auf dem Remote-Gerät.
- In einer Datei mit der Erweiterung syslog, die sich im Ordner des Administrationsagenten auf dem Remote-Gerät befindet (beispielsweise C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- In der Ereignisdatenbank von Kaspersky Security Center.

Verbindung des Client-Geräts mit dem Administrationsserver prüfen

Kaspersky Security Center ermöglicht eine automatische oder manuelle Überprüfung der Verbindungen zwischen einem Client-Gerät und dem Administrationsserver.

Die automatische Überprüfung der Verbindung erfolgt auf dem Administrationsserver. Die manuelle Überprüfung der Verbindung erfolgt auf dem Gerät.

Verbindung des Client-Geräts mit dem Administrationsserver automatisch prüfen

Um die automatische Überprüfung der Verbindung zwischen einem Client-Gerät und dem Administrationsserver auszuführen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die entsprechende Administrationsgruppe des Geräts aus.
2. Wählen Sie im Arbeitsbereich der Administrationsgruppe auf der Registerkarte **Geräte** das gewünschte Gerät aus.
3. Wählen Sie im Kontextmenü des Geräts den Punkt **Verfügbarkeit des Geräts prüfen** aus.

Im folgenden Fenster werden Daten über die Verfügbarkeit des Geräts angezeigt.

Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk

Sie können die Verbindung zwischen einem Client-Gerät und dem Administrationsserver mit dem Tool "klnagchk" überprüfen. Darüber hinaus können Sie mit dem Tool ausführliche Informationen über die Verbindungseinstellungen zwischen dem Client-Gerät und dem Administrationsserver erhalten. Das Tool "klnagchk" befindet sich im Installationsordner des Administrationsagenten.

Beim Starten über die Befehlszeile führt das Tool "klnagchk" je nach Parameter die folgenden Aktionen aus:

- Es zeigt eine Meldung auf dem Bildschirm an oder nimmt eine Eintragung in der Log-Datei der Einstellungswerte für die Verbindung vor, die zwischen dem Administrationsagenten des Geräts und dem Administrationsserver besteht.
- Es trägt in einer Ereignisprotokolldatei die Statistik des Administrationsagenten (beginnend mit dessen letztem Start) und die Ausführungsergebnisse des Tools ein, oder es gibt diese Informationen auf dem Bildschirm aus.
- Es versucht eine Verbindung zwischen dem Administrationsagenten und Administrationsserver herzustellen.

  Bei fehlgeschlagenem Verbindungsaufbau sendet das Tool ein ICMP-Paket an das Gerät, um den Status des Geräts zu überprüfen, auf dem der Administrationsserver installiert ist.

So prüfen Sie die Verbindung zwischen einem Client-Gerät und dem Administrationsserver mit dem Tool "klnagchk":

Starten Sie auf dem Gerät mit installiertem Administrationsagenten das Tool "klnagchk" über die Befehlszeile und unter Verwendung eines lokalen Administratorkontos.

Die Befehlszeilensyntax des Tools lautet:

```
klnagchk [-logfile <Dateiname>] [-sp] [-savecert <Pfad zur Zertifikatsdatei>] [-
restart][-sendhb]
```

Beschreibung der Parameter:

- `-logfile <Dateiname>` – Schreibt die Parameterwerte für die Verbindung zwischen Administrationsagenten und Administrationsserver sowie die Ausführungsergebnisse des Tools in eine Protokolldatei.

  Standardmäßig werden diese Informationen im Standardausgabe-Stream (stdout) gespeichert. Wenn das Argument nicht verwendet wird, werden die Einstellungen, Ergebnisse und Fehlermeldungen auf dem Bildschirm ausgegeben.

- `-sp` – Zeigt bei der Ausgabe das Kennwort für Authentifizierung des Benutzers am Proxy-Server.

  Dieses Argument wird verwendet, wenn die Verbindung zum Administrationsserver über einen Proxy-Server aufgebaut wird.

- `-savecert <Dateiname>` – Speichert das Zertifikat für den Zugriff auf den Administrationsserver in der angegebenen Datei.

- `-restart` – Startet den Administrationsagenten nach Abschluss des Tools.

- `-sendhb` – Startet die Synchronisation des Administrationsagenten mit dem Administrationsserver.

Nach dem Start greift das Tool "klnagchk" auf die Konfigurationsdateien des Administrationsagenten zu und zeigt die Verbindungsparameter an. Die folgenden Parameter werden während der Installation des Administrationsagenten und in den Einstellungen der Richtlinie des Administrationsagenten angegeben:

- `Current device` – Name des Client-Geräts im Windows-Netzwerk

- `Network Agent version` – Vollständige Versionsnummer des auf dem Gerät installierten Administrationsagenten (mit Patches)

- `Administration Server address` – Adresse des Administrationsservers

- `Use SSL` – Parameter zur Angabe, ob die Verbindung mit dem Administrationsserver gesichert ist

  Mögliche Werte:

  - 0 – Es wird keine sichere Verbindung verwendet.

  - 1 – Es wird eine sichere Verbindung verwendet.

- `Compress traffic` – Parameter zur Angabe, ob der Datenverkehr zwischen dem Client-Gerät und dem Administrationsserver komprimiert wird

- `Numbers of the Administration Server SSL ports` – Nummern der gültigen Ports für die Kommunikation mit dem Administrationsserver, wenn eine sichere Verbindung verwendet wird.

- `Numbers of the Administration Server ports` – Anzahl der gültigen Ports für die Kommunikation mit dem Administrationsserver, wenn eine normale Verbindung verwendet wird.

- `Use proxy server` – Parameter zur Angabe, ob ein Proxyserver verwendet wird

Mögliche Werte:

- 0 – Es wird kein Proxyserver verwendet.
- 1 – Es wird ein Proxyserver verwendet.

- `Address` – Adresse und Port des Proxyservers, getrennt durch einen Doppelpunkt. Dieser Parameter wird nur angezeigt, wenn ein Proxyserver verwendet wird.
- `User name` – Benutzername für den Zugriff auf den Proxyserver. Dieser Parameter wird nur angezeigt, wenn ein Proxyserver verwendet wird.
- `Password` – Kennwort für den Zugriff auf den Proxyserver. Dieser Parameter wird nur angezeigt, wenn ein Proxyserver verwendet wird. Um das Kennwort des Proxyservers anzuzeigen, müssen Sie im Befehl das Argument `sp` angeben.
- `Administration Server certificate` – Parameter zur Angabe, ob das Client-Gerät über ein Zertifikat des Administrationsservers verfügt. Es kann beispielsweise vorkommen, das kein Zertifikat vorhanden ist, wenn sich der Administrationsagent noch nie erfolgreich mit dem Administrationsserver verbunden hat.

  Mögliche Werte:

  - `not installed` – Das Client-Gerät besitzt kein Zertifikat des Administrationsservers.
  - `available` –Das Client-Gerät besitzt ein Zertifikat des Administrationsservers.
- `Open UDP port` – Parameter zur Angabe, ob der Administrationsagent den UDP-Port verwendet, um Synchronisierungsanfragen vom Administrationsserver zu empfangen.

  Mögliche Werte:

  - 0 – Der UDP-Port ist für den Empfang von Synchronisationsanfragen vom Administrationsserver geschlossen.
  - 1 – Der UDP-Port ist für den Empfang von Synchronisationsanfragen vom Administrationsserver geöffnet.
- `Numbers of UDP ports` – Nummern der UDP-Ports, die vom Administrationsagenten verwendet werden können.
- `Location name` – Netzwerkstandort des Geräts.
- `State of network location` – Parameter zu Angabe, ob auf dem Client-Gerät von einem Administrationsserver-Verbindungsprofil auf ein anderes gewechselt werden kann.

  Mögliche Werte:

  - `Enabled` – Das Administrationsserver-Verbindungsprofil kann für das Client-Gerät gewechselt werden.
  - `Disabled` – Das Administrationsserver-Verbindungsprofil kann für das Client-Gerät nicht gewechselt werden.
- `Profile to use` – Verbindungsprofil für den Administrationsserver.
- `Condition` – IP-Adresse und Subnetzmaske des Netzwerks, mit dem das Client-Gerät verbunden ist.
- `Synchronization interval (min)` –Standardintervall zwischen Synchronisierungen.

- `Connection timeout (in seconds)` – Timeout für die Verbindung.
- `Send / receive timeout (in seconds)` – Timeout für die Verbindung von Lese-/Schreibvorgängen.
- `Device ID` – Geräte-ID im Netzwerk. Die `Device ID` ist für jedes Client-Gerät eindeutig, das von einem bestimmten Administrationsserver verwaltet wird.
- `Locations of connection gateways` – Parameter für die Verbindung des Client-Geräts mit dem Administrationsserver über das Verbindungs-Gateway.
- `Location of distribution points` – Parameter für die Verbindung des Client-Geräts mit dem Administrationsserver über den Verteilungspunkt.
- `Connection with server` –Parameter zur Angabe, ob das Verbindungs-Gateway eine dauerhafte Verbindung zum Administrationsserver unterhält. Der Parameter wird nur angezeigt, wenn das Client-Gerät als Verbindungs-Gateway agiert.

  Mögliche Werte:

  - `active` – Das Verbindungs-Gateway unterhält eine dauerhafte Verbindung zum Administrationsserver.
  - `inactive` – Das Verbindungs-Gateway unterhält keine dauerhafte Verbindung zum Administrationsserver.
- `Connection with server through connection gateway` – Parameter zur Angabe, ob die Verbindung zum Administrationsserver über ein Verbindungs-Gateway korrekt hergestellt wurde. Der Parameter wird nur angezeigt, wenn das Client-Gerät als Verbindungs-Gateway agiert.

  Mögliche Werte:

  - `active` – Die Verbindung zum Administrationsserver über ein Verbindungs-Gateway wurde ordnungsgemäß hergestellt.
  - `inactive` – Die Verbindung zum Administrationsserver über ein Verbindungs-Gateway wurde nicht ordnungsgemäß hergestellt.

Darüber hinaus kann die Ausgabe des Tools "klnagchk" eine der folgenden Zeilen enthalten:

- `Administration Server is installed on this device` – Das Tool "klnagchk" wird auf dem Gerät mit dem Administrationsserver ausgeführt.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – Das Tool "klnagchk" wird auf einem Gerät ausgeführt, auf dem der Administrationsagent im Verbindungs-Gateway-Modus installiert ist. Das konfigurierte Verbindungs-Gateway wartet auf eine Verbindung vom Administrationsserver, aber dieser listet das Gerät nicht unter den verwalteten Geräten auf. Sie müssen sicherstellen, dass der Administrationsserver eine Verbindung zu dem Verbindungs-Gateway initiiert.
- `This device is a connection gateway` –Das Tool "klnagchk" wird auf einem Gerät ausgeführt, das als Verbindungs-Gateway agiert.
- `Acts as a distribution point` – Das Tool "klnagchk" wird auf einem Gerät ausgeführt, das als Verteilungspunkt agiert.

Das Tool "klnagchk" überprüft den Status des Dienstes des Administrationsagenten. Wird dieser Dienst nicht ausgeführt, wird das Tool beendet. Wenn der Dienst ausgeführt wird, zeigt das Tool die folgenden Verbindungsstatistiken an:

- `Total number of synchronization requests` – Anzahl der Versuche, eine Verbindung des Client-Geräts mit dem Administrationsserver herzustellen.
- `The number of successful synchronization request` – Anzahl der erfolgreichen Versuche, eine Verbindung des Client-Geräts mit dem Administrationsserver herzustellen.
- `Total number of synchronizations` – Anzahl der Versuche, die Einstellungen des Client-Geräts mit den Einstellungen des Administrationsservers zu synchronisieren.
- `The number of successful synchronizations` – Anzahl der erfolgreichen Versuche, die Einstellungen des Client-Geräts mit dem Administrationsserver zu synchronisieren.
- `Date/time of the last request for synchronization` – Datum und Uhrzeit der letzten Verbindung.

Um die Verbindung zwischen dem Administrationsserver und dem Administrationsagenten zu analysieren, müssen Sie die Parameter `Total number of synchronization requests` und `The number of successful synchronization request` verwenden. Die Einstellungen des Client-Geräts werden nur dann mit den Einstellungen des Administrationsservers synchronisiert, wenn sich die Einstellungen des Administrationsservers geändert haben (z. B. wenn neue Aufgaben hinzugefügt oder Richtlinieneinstellungen geändert wurden). Andernfalls bleiben die Parameterwerte `Total number of synchronizations` und `The number of successful synchronizations` unverändert.

Weitere Informationen zur Behebung von Verbindungsproblemen zwischen Administrationsagenten und Administrationsserver finden Sie in den FAQ zu Kaspersky Security Center.

Über das Überprüfen der Verbindungszeit des Geräts mit dem Administrationsserver

Wenn ein Gerät heruntergefahren wird, benachrichtigt der Administrationsagent den Administrationsserver über dieses Ereignis. In der Verwaltungskonsole wird das Gerät als heruntergefahren angezeigt. Der Administrationsagent kann den Administrationsserver jedoch nicht über alle derartigen Ereignisse benachrichtigen. Der Administrationsserver analysiert deshalb periodisch das Attribut **Verbindung mit dem Administrationsserver** (Dieser Wert des Attributs wird in der Verwaltungskonsole in den Geräteeigenschaften im Abschnitt **Allgemein** angezeigt) für jedes Gerät und vergleicht es mit dem Synchronisierungsintervall aus den aktuellen Einstellungen des Administrationsagenten. Wenn ein Gerät über mehr als drei aufeinander folgende Synchronisationsintervalle nicht reagiert hat, wird dieses Gerät als abgeschaltet markiert.

Client-Geräte auf dem Administrationsserver identifizieren

Die Client-Geräte werden anhand ihrer Namen identifiziert. Der Name des Geräts ist einzigartig unter allen Namen der Geräte, die mit dem Administrationsserver verbunden sind.

Der Name des Geräts wird beim Durchsuchen des Windows-Netzwerks und beim Erkennen eines neuen Geräts oder beim ersten Verbindungsaufbau des auf dem Gerät installierten Administrationsagenten zum Administrationsserver an den Server weitergegeben. Standardmäßig stimmt der Name mit dem Namen des Geräts im Windows-Netzwerk (NetBIOS-Name) überein. Wenn auf dem Administrationsserver ein Gerät mit dem gleichen Namen bereits registriert ist, wird dem neuen Gerät eine Endung mit einer Ordnungszahl wie **<Name>-1**, **<Name>-2** hinzugefügt. Unter diesem Namen wird das Gerät in die Administrationsgruppe übernommen.

Verschieben von Geräten zu Administrationsgruppe

Sie können Geräte von einer Administrationsgruppe in eine andere verschieben, wenn Sie über die Berechtigung **Ändern** im Bereich **Verwaltung von Administrationsgruppen** sowohl für Administrationsquellgruppen als auch Administrationszielgruppen (oder für den Administrationsserver, zu dem diese Gruppen gehören) verfügen.

Um eines oder mehrere Geräte zu einer gewählten Administrationsgruppe hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte**.
2. Wählen Sie im Ordner **Verwaltete Geräte** den Unterordner aus, welcher der Gruppe entspricht, in der die Client-Geräte aufgenommen werden sollen.

   Wenn Geräte zur Gruppe **Verwaltete Geräte** hinzugefügt werden sollen, können Sie diesen Schritt überspringen.
3. Um Geräte zu einer Gruppe hinzuzufügen, führen Sie im Arbeitsbereich der gewählten Administrationsgruppe auf der Registerkarte **Geräte** einer der folgenden Optionen aus:

   - Klicken Sie im Informationsfeld mit der Geräteliste auf den Link **Geräte in Gruppe verschieben**
   - Klicken Sie mit der rechten Maustaste auf die Liste der Geräte und wählen **Erstellen → Gerät** aus

   Daraufhin wird der Assistent für das Verschieben von Geräten gestartet. Folgen Sie den Anweisungen. Legen Sie dabei fest, wie die Geräte zur Gruppe verschoben werden sollen, und erstellen Sie eine Liste der Geräte, die zu der Gruppe gehören.

   Wenn Sie die Geräteliste manuell erstellen, können Sie als Gerätadresse die IP-Adresse (bzw. das IP-Intervall), den NetBIOS- bzw. DNS-Namen verwenden. Manuell können zur Geräteliste nur die Geräte verschoben werden, deren Informationen bei der Verbindung mit dem Gerät oder nach einer Gerätesuche in die Administrationsserver-Datenbank bereits eingetragen wurden.

   Um die Geräteliste aus einer Datei zu importieren, geben sie die TXT-Datei mit dem Verzeichnis der Adressen für Geräte, die hinzugefügt werden sollen. Dabei muss jede Adresse in einer separaten Zeile aufgeführt sein.

Nach Abschluss des Assistenten werden die gewählten Geräte in die Administrationsgruppe aufgenommen und in der Geräteliste mit den Namen angezeigt, die der Administrationsserver bestimmt hat.

Sie können ein Gerät in die ausgewählte Administrationsgruppe verschieben, indem Sie es mit der Maus aus dem Ordner **Nicht zugeordnete Geräte** in den Ordner dieser Administrationsgruppe ziehen.

Administrationsserver für Client-Geräte wechseln

Sie können den Administrationsserver, der die Client-Geräte verwaltet, durch einen anderen Administrationsserver mit der Aufgabe *Administrationsserver wechseln* ersetzen.

Um einen Administrationsserver, der die Client-Geräte verwaltet, zu wechseln, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Starten Sie mithilfe der Schaltfläche **Neue Aufgabe** im Arbeitsbereich des Ordners den Assistenten für die Erstellung von Aufgaben.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.

3. Wählen Sie im Schritt **Aufgabentyp auswählen** des Assistenten den Knoten **Kaspersky Security Center Administrationsserver**, öffnen Sie den Ordner **Erweitert** und wählen Sie anschließend die Aufgabe **Administrationsserver wechseln**.

4. Klicken Sie im neuen Fenster auf die Schaltfläche **OK**, um die Bedingungen für das Wechseln des Administrationsservers für Client-Geräte zu akzeptieren.

5. Wählen Sie im Schritt **Einstellungen** des Assistenten den Administrationsserver aus, den Sie für die Verwaltung der ausgewählten Geräte verwenden möchten:

   - **Zu einem anderen primären Administrationsserver wechseln**

     Um Client-Geräte auf einen anderen primären Administrationsserver zu verschieben, geben Sie die folgenden Verbindungseinstellungen für den Administrationsserver an:

     1. Geben Sie im Feld **Administrationsserver** die Adresse des neuen primären Administrationsservers an.

     2. Geben Sie im Feld **Port** die Portnummer für die Verbindung zum Administrationsserver an.

        Standardmäßig wird die Portnummer 14000 verwendet.

     3. Geben Sie im Feld **SSL-Port** die Nummer des SSL-Ports auf dem primären Administrationsserver an

        Standardmäßig wird die Portnummer 13000 verwendet.

     4. Aktivieren Sie bei Bedarf das Kontrollkästchen **Proxyserver verwenden**.

        Wenn dieses Kontrollkästchen deaktiviert ist, wird die direkte Verbindung genutzt, um das Gerät mit dem Administrationsserver zu verbinden.

        Wenn diese Kontrollkästchen aktiviert ist, geben Sie die Parameter des Proxyservers an:

        - **Proxyserver-Adresse**

        - **Proxyserver-Port**

        Falls Ihr Proxyserver eine Authentifizierung erfordert, geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldeinformationen des Kontos ein, unter dem die Verbindung mit dem Proxyserver hergestellt wird. Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

     5. Laden Sie bei Bedarf ein neues Zertifikat für den Administrationsserver hoch.

   - **Zu einem anderen virtuellen Server auf diesem primären Server wechseln**

     Wählen Sie diese Option aus, um die Client-Geräte zu einem virtuellen Administrationsserver auf dem aktuellen primären Administrationsserver verschieben. Geben Sie dazu im Feld **Name des virtuellen Administrationsservers** den Namen des erforderlichen virtuellen Administrationsservers an.

Geben Sie bei Bedarf die Wartezeit an, bevor der Administrationsagent neu gestartet wird.

6. Wählen Sie in diesem Schritt des Assistenten die Geräte aus, denen die Aufgabe zugewiesen wird:

   - **Geräte auswählen, die vom Administrationsserver erkannt wurden**. In diesem Fall wird die Aufgabe einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

   - **Geräteadressen manuell angeben oder aus Liste importieren** Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

   - **Aufgabe einer Geräteauswahl zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine vordefinierte Auswahl oder Ihre eigene Auswahl angeben.

   - **Aufgabe einer Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu der zuvor erstellten Administrationsgruppe gehören.

7. Geben Sie im Schritt **Benutzerkonto für die Ausführung der Aufgabe auswählen** des Assistenten die Kontoeinstellungen an:

   - **Standardbenutzerkonto**

     Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

     Diese Variante ist standardmäßig ausgewählt.

   - **Benutzerkonto festlegen**

     Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

     - **Benutzerkonto**

       Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

     - **Kennwort**

       Kennwort des Benutzerkontos, unter dem die Aufgabe ausgeführt wird.

8. Im Schritt **Aufgabenzeitplan anpassen** des Assistenten können Sie einen Zeitplan für den Aufgabenstart erstellen. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **Start nach Zeitplan:**

     Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

     - **Täglich (Sommerzeit wird nicht unterstützt)**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

       Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Rückwärtskompatibilität von Kaspersky Security Center benötigt.

Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Einmal**

  Die Aufgabe wird einmal zum angegebenen Datum und zur angegebenen Uhrzeit ausgeführt (standardmäßig entspricht dies dem Tag, an dem die Aufgabe erstellt wurde).

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Sofort**

  Die Aufgabe wird sofort ausgeführt, sobald das Gerät im Netzwerk sichtbar wird oder sobald das Gerät in den Gültigkeitsbereich der Aufgabe aufgenommen wird.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

9. Geben Sie in diesem Schritt des Assistenten den Namen der Aufgabe an, die Sie erstellen.

10. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um den Assistenten abzuschließen.

    Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe unmittelbar nach Abschluss des Assistenten gestartet wird.

Nach Abschluss der Aufgabe werden die Client-Geräte, für welche die Aufgabe erstellt wurde, auf den Administrationsserver umgestellt, der in den Einstellungen der Aufgabe angegeben wurde.

Wenn der Administrationsserver Verschlüsselung und Datenschutz unterstützt und Sie eine Aufgabe *Administrationsserver wechseln* erstellen, wird eine Warnung angezeigt. Die Warnung besagt, dass für den Fall, dass verschlüsselte Daten auf Geräten gespeichert werden, nachdem der neue Server mit der Verwaltung der Geräte beginnt, Benutzer nur auf die verschlüsselten Daten zugreifen können, mit denen sie zuvor gearbeitet haben. In anderen Fällen werden die Daten nicht freigegeben. Eine ausführliche Beschreibung der Fälle, in denen die verschlüsselten Daten nicht freigegeben werden, können Sie der Hilfe von Kaspersky Endpoint Security für Windows entnehmen.

Geräte, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind, auf einen anderen Administrationsserver verschieben

Sie können Geräte, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind, auf einen anderen Administrationsserver verschieben. Dies kann beispielsweise erforderlich sein, wenn Sie eine andere Version des Administrationsservers installieren und dabei den Administrationsagenten auf den Geräten nicht erneut installieren möchten, um Zeit zu sparen.

Die in dieser Anleitung beschriebenen Befehle müssen auf Client-Geräten unter einem Benutzerkonto mit Administratorrechten ausgeführt werden.

So verschieben Sie ein Gerät, das über das Verbindungs-Gateway verbunden ist, auf einen anderen Administrationsserver:

1. Starten Sie das Tool klmover mit dem Parameter `-address < Serveradresse >`, um zu dem neuen Administrationsserver zu wechseln.

2. Führen Sie den Befehl `klnagchk -nagwait -tl 4` aus.

3. Führen Sie die folgenden Befehle aus, um ein neues Verbindungs-Gateway anzugeben:

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<IP oder Name des Gateways>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `<IP oder Name des Gateways>` entspricht hier der Adresse des Verbindungs-Gateways, mit der über das Internet auf das Gateway zugegriffen werden kann.

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` steht für die Nummer des TCP-Ports, der das Verbindungs-Gateway überwacht.

4. Führen Sie den Befehl `klnagchk -restart -tl 4` aus, um den Dienst des Administrationsagenten zu starten.

Das Gerät wird auf den neuen Administrationsserver verschoben und über das neue verbundene Gateway verbunden.

Server-Cluster und -Arrays

Kaspersky Security Center unterstützt die Cluster-Technologie. Sobald der Administrationsserver vom Administrationsagenten die Information erhält, dass ein auf einem Client-Gerät installiertes Programm zum Server-Array gehört, wird das betreffende Client-Gerät als Knoten in dem Cluster eingebunden. Der Cluster wird in der Konsolenstruktur mit dem Server-Symbol () im Ordner **Verwaltete Geräte** als separates Objekt hinzugefügt.

Cluster weisen folgende typische Merkmale auf:

- Ein Cluster und alle seine Knoten befinden sich stets in derselben Administrationsgruppe.
- Versucht der Administrator, einen Knoten eines Clusters zu verschieben, kehrt dieser automatisch wieder an seine ursprüngliche Position zurück.
- Versucht der Administrator, einen Knoten eines Clusters in eine andere Gruppe zu verschieben, so werden sämtliche Knoten des Clusters in die betreffende Gruppe verschoben.

Client-Geräte von einem entfernten Standort einschalten, ausschalten und Neustart durchführen

Kaspersky Security Center ermöglicht die Remoteverwaltung (Einschalten, Ausschalten und Neustarten) von Client-Geräten.

Um Client-Geräte im Remote-Betrieb zu verwalten, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die Geräte verwaltet.
2. Erstellen Sie eine Aufgabe zur Verwaltung eines Geräts auf eine der folgenden Arten:
   - Wenn es erforderlich ist, die zur gewählten Administrationsgruppe gehörenden Geräte einzuschalten, auszuschalten oder neu zu starten, erstellen Sie eine Aufgabe für die gewählte Gruppe.
   - Wenn es erforderlich ist, zu unterschiedlichen Administrationsgruppen gehörende Geräte einzuschalten, auszuschalten oder neu zu starten, erstellen Sie eine Aufgabe für eine Reihe von Geräten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten für das Erstellen einer Aufgabe den Knoten **Kaspersky Security Center** aus, öffnen Sie den Ordner **Erweitert** und wählen Sie die Aufgabe **Verwaltung der Geräte** aus.
3. Starten Sie die erstellte Aufgabe.

   Nach Abschluss der Aufgabe wird der Befehl (Einschalten, Ausschalten oder Neu starten) auf den ausgewählten Geräten ausgeführt.

Über die Verwendung einer dauerhaften Verbindung zwischen dem verwalteten Gerät und dem Administrationsserver

Standardmäßig gibt es in Kaspersky Security Center keine ständigen Verbindungen zwischen den verwalteten Geräten und dem Administrationsserver. Die Administrationsagenten auf den verwalteten Geräten stellen regelmäßig eine Verbindung mit dem Administrationsserver her und führen eine Synchronisierung durch. Das Intervall zwischen den Synchronisierungs-Sessions wird durch die Richtlinie des Administrationsagenten vorgegeben und beträgt standardmäßig 15 Minuten. Wenn eine vorzeitige Synchronisierung (beispielsweise zur Beschleunigung der Anwendung einer Richtlinie) erforderlich ist, sendet der Administrationsserver dem Administrationsagenten ein signiertes Netzwerkpaket an den UDP-Port 15000 (Der Administrationsserver kann das Paket über IPv4- oder IPv6-Netzwerke versenden). Wenn aus einem bestimmten Grund keine Verbindung vom Administrationsserver zum verwalteten Gerät über UDP möglich ist, wird die Synchronisierung bei der nächsten regelmäßigen Verbindung des Administrationsagenten mit dem Administrationsserver im Laufe des Synchronisierungsintervalls durchgeführt.

Einige Vorgänge können ohne eine frühzeitige Verbindung zwischen dem Administrationsagenten und dem Administrationsserver jedoch nicht ausgeführt werden. Diese Vorgänge umfassen das Starten und Stoppen von lokalen Aufgaben, das Empfangen von Statistiken für verwaltete Geräte und der Herstellen eines Tunnels. Um diese Vorgänge zu ermöglichen, müssen Sie die Option **Verbindung mit Administrationsserver nicht trennen** auf dem verwalteten Gerät aktivieren.

Über erzwungene Synchronisierung

Obwohl Kaspersky Security Center den Status, die Einstellungen, die Aufgaben und die Richtlinien für die verwalteten Geräte automatisch synchronisiert, muss der Administrator in einzelnen Fällen genau wissen, ob an diesem Moment für ein bestimmtes Gerät die Synchronisierung ausgeführt worden ist.

Das Kontextmenü der verwalteten Geräte in der Verwaltungskonsole enthält im Menüpunkt **Alle Aufgaben** den Befehl **Synchronisierung erzwingen**. Wenn Kaspersky Security Center 15.1 diesen Befehl ausführt, versucht der Administrationsserver, eine Verbindung zum Gerät herzustellen. Ist dieser Versuch erfolgreich, so wird die Synchronisierung erzwungen. Andernfalls erfolgt die erzwungene Synchronisierung erst nach der nächsten geplanten Verbindung des Administrationsagenten mit dem Administrationsserver.

Über den Zeitplan der Verbindung

Im Eigenschaftenfenster der Richtlinie des Administrationsagenten, im untergeordneten Abschnitt **Verbindungszeitplan** des Abschnitts **Konnektivität** können Sie die Zeitintervalle für die Übermittlung von Daten an den Administrationsserver durch den Administrationsagenten festlegen.

Verbindung bei Bedarf herstellen. Bei dieser Variante wird eine Verbindung dann hergestellt, wenn Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen.

Verbindung in den angegebenen Zeiträumen herstellen. Bei dieser Variante wird eine Verbindung des Administrationsagenten mit dem Administrationsserver in den vorgegebenen Zeiträumen hergestellt. Sie können mehrere Zeiträume für die Verbindung hinzufügen.

Nachricht an Gerätenutzer senden

Um eine Nachricht an Gerätenutzer zu senden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Erstellen Sie eine Aufgabe für das Senden einer Nachricht an Gerätenutzer auf eine der folgenden Arten:
   - Wenn es erforderlich ist, eine Meldung an die Benutzer der Geräte zu senden, die zur gewählten Administrationsgruppe gehören, erstellen Sie eine Aufgabe für die gewählte Gruppe.
   - Wenn Sie eine Meldung an die Benutzer der Geräte senden möchten, die zu unterschiedlichen oder zu keinen Administrationsgruppen gehören, erstellen Sie eine Aufgabe für eine Reihe von Geräten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.
3. Wählen Sie im Fenster "Aufgabentyp" des Assistenten für das Erstellen einer Aufgabe den Knoten **Kaspersky Security Center Administrationsserver** aus, öffnen Sie den Ordner **Erweitert** und wählen Sie die Aufgabe **Benutzernachricht** aus. Die Aufgabe Nachrichten an Benutzer senden ist nur für Geräte verfügbar, die unter Windows laufen. Sie können auch Nachrichten im Kontextmenü des Benutzers im Ordner **Benutzerkonten** senden.
4. Starten Sie die erstellte Aufgabe.

   Nach Abschluss der Aufgabe wird die Nachricht an die Benutzer der gewählten Geräte gesendet. Die Aufgabe Nachrichten an Benutzer senden ist nur für Geräte verfügbar, die unter Windows laufen. Sie können auch Nachrichten im Kontextmenü des Benutzers im Ordner **Benutzerkonten** senden.

Arbeit mit dem Programm Kaspersky Security for Virtualization

Kaspersky Security Center unterstützt die Möglichkeit, virtuelle Maschinen mit dem Administrationsserver zu verbinden. Der Schutz von virtuellen Maschinen erfolgt mit dem Programm Kaspersky Security for Virtualization. Weitere Informationen entnehmen Sie bitte der Dokumentation zu diesem Programm.

Wechsel der Statuswerte von Geräten konfigurieren

Sie können die Bedingungen ändern, um einem Gerät den Status *Kritisch* oder *Warnung* zuzuweisen.

Um die Änderungen des Gerätestatus auf Kritisch zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftenfenster auf eine der folgenden Arten:

   - Wählen Sie im Ordner **Richtlinien** im Kontextmenü der Richtlinie eines Administrationsservers **Eigenschaften** aus.

   - Wählen Sie im Kontextmenü einer Administrationsgruppe den Punkt **Eigenschaften** aus.

2. Wählen Sie im nächsten Fenster **Eigenschaften** im Bereich **Abschnitte** den Punkt **Gerätestatus** aus.

3. Aktivieren Sie im rechten Bereich im Abschnitt **Werte mit Status "Kritisch"** das Kontrollkästchen neben einer Bedingung in der Liste.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

4. Doppelklicken Sie auf den Namen der ausgewählten Bedingung und legen Sie anschließend im neuen Fenster den erforderlichen Wert für die Bedingung fest.

   Für die folgenden Bedingungen können Sie keine Werte festlegen: Es wurde keine Sicherheitsanwendung installiert, Es sind inkompatible Programme installiert, Es wurden Schwachstellen in Programmen erkannt, Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie, Es wurden unbearbeitete Sicherheitsprobleme erkannt, Gerätestatus wird vom Programm bestimmt, Das Gerät wird nicht mehr verwaltet, Die Sicherheitsanwendung wurde nicht gestartet, Lizenz abgelaufen.

   Für die Bedingung **Neustart erforderlich** können Sie die Gründe für den Neustart angeben. Es wird empfohlen, die Kontrollkästchen für alle Gründen in der Liste zu aktivieren.

5. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftenfenster auf eine der folgenden Weisen:

   - Wählen Sie im Ordner **Richtlinien** im Kontextmenü der Richtlinie des Administrationsservers den Punkt **Eigenschaften** aus.

   - Wählen Sie im Kontextmenü der Administrationsgruppe den Punkt **Eigenschaften** aus.

2. Wählen Sie im nächsten Fenster **Eigenschaften** im Bereich **Abschnitte** den Punkt **Gerätestatus** aus.

3. Aktivieren Sie im rechten Bereich im Abschnitt **Werte mit Status "Warnung"** das Kontrollkästchen neben einer Bedingung in der Liste.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

4. Doppelklicken Sie auf den Namen der ausgewählten Bedingung und legen Sie anschließend im neuen Fenster den erforderlichen Wert für die Bedingung fest.

   Für die folgenden Bedingungen können Sie keine Werte festlegen: Es wurde keine Sicherheitsanwendung installiert, Es sind inkompatible Programme installiert, Es wurden Schwachstellen in Programmen erkannt, Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie, Es wurden unbearbeitete Sicherheitsprobleme erkannt, Gerätestatus wird vom Programm bestimmt, Das Gerät wird nicht mehr verwaltet, Die Sicherheitsanwendung wurde nicht gestartet, Lizenz abgelaufen.

   Für die Bedingung **Neustart erforderlich** können Sie die Gründe für den Neustart angeben. Es wird empfohlen, die Kontrollkästchen für alle Gründen in der Liste zu aktivieren.

5. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Zuweisung von Tags an die Geräte die Anzeige der zugewiesenen Tags

Kaspersky Security Center erlaubt, den Geräten Tags zuzuweisen. Ein *Tag* stellt eine ID des Geräts dar, die für die Gruppierung, Beschreibung oder Suche der Geräte verwendet werden kann. Die den Geräten zugewiesenen Tags können beim Erstellen von Geräteauswahlen, bei der Suche nach Geräten und bei der Gerätezuordnung anhand von Administrationsgruppen verwendet werden.

Die Tags können den Geräten manuell oder automatisch zugewiesen werden. Die manuelle Zuweisung von Tags zu einem Gerät wird in den Eigenschaften des Geräts ausgeführt und kann erforderlich sein, wenn ein einzelnes Gerät markiert muss. Die automatische Zuweisung der Tags wird vom Administrationsserver entsprechend den festgelegten Regeln zur Zuweisung von Tags ausgeführt.

In den Eigenschaften des Administrationsservers können Sie die automatische Zuweisung von Tags an die von diesem Administrationsserver verwalteten Geräte anpassen. Die automatische Bestimmung der Tags an die Geräte erfolgt beim Ausführen bestimmter Regeln. Jedem Tag entspricht eine separate Regel. Die Regeln können auf die Netzwerkeigenschaften des Geräts, das Betriebssystem, die auf dem Gerät installierten Programmen und andere Eigenschaften des Geräts angewendet werden. Beispielsweise können Sie eine Regel konfigurieren, gemäß der Geräten, die unter Verwaltung des Betriebssystems Windows arbeiten, das Tag *Win* zugewiesen wird. Dieses Tag kann dann beim Erstellen von Geräteauswahlen verwendet werden, um Geräte auszuwählen, die unter Verwaltung des Betriebssystems Windows arbeiten, und ihnen eine Aufgabe zuzuweisen.

Sie können Tags auch als Bedingung für die Aktivierung eines Richtlinienprofils auf dem verwalteten Gerät verwenden, damit bestimmte Richtlinienprofile nur auf Geräten verwendet werden, die bestimmte Tags haben. Wenn beispielsweise in der Administrationsgruppe *Benutzer* das Gerät mit dem Tag *Kurier* erscheint und für das Tag *Kurier* die Aktivierung des entsprechenden Richtlinienprofils konfiguriert ist, wird auf diesem Gerät nicht die für die Gruppe *Benutzer* erstellte Richtlinie selbst, sondern ihr Profil angewendet. Das Richtlinienprofil kann auf diesem Gerät den Start einzelner Programme erlauben, deren Start im Rahmen der Richtlinie verboten ist.

Sie können mehrere Regeln zur Zuweisung von Tags erstellen. Einem Gerät können mehrere Tags zugewiesen werden, falls Sie mehrere Regeln zur Zuweisung von Tags erstellt haben und Bedingungen dieser Regeln gleichzeitig erfüllt sind. Sie können die Liste aller zugewiesenen Tags in den Eigenschaften des Geräts einsehen. Jede Regel zur Zuweisung von Tags kann aktiviert oder deaktiviert werden. Wenn die Regel aktiviert ist, wird sie auf den Geräten angewendet, die vom Administrationsserver verwaltet werden. Wenn eine Regel nicht notwendig ist, aber eventuell in Zukunft benötigt wird, muss sie nicht gelöscht werden; es genügt, das Kontrollkästchen **Regel aktivieren** zu deaktivieren. Dadurch wird die Regel deaktiviert und solange nicht ausgeführt, wie das Kontrollkästchen **Regel aktivieren** deaktiviert ist. Das Deaktivieren der Regel ohne Löschen kann erforderlich sein, wenn diese Regel vorübergehend aus der Liste der Regeln zur Zuweisung von Tags ausgeschlossen werden muss und später wieder aktiviert werden soll.

Geräten automatisch Tags zuweisen

Sie können Regeln zur automatischen Zuweisung von Tags im Eigenschaftenfenster des Administrationsservers erstellen und ändern.

Um den Geräten automatisch Tags zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Knoten mit dem Namen des Administrationsservers aus, für den die Regeln zur Zuweisung von Tags festgelegt werden sollen.

2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Regeln zur Zuweisung von Tags** aus.

4. Klicken Sie im Abschnitt **Regeln zur Zuweisung von Tags** auf **Hinzufügen**.

   Das Fenster **Neue Regel** wird geöffnet.

5. Passen Sie im Fenster **Neue Regel** die allgemeinen Eigenschaften der Regel an:

   - Geben Sie den Namen der Regel an.

     Der Name der Regel darf nicht mehr als 255 Zeichen umfassen und keine Sonderzeiten (wie `"*<>?\:|`) enthalten.

   - Aktivieren bzw. deaktivieren Sie die Regel mithilfe des Kontrollkästchens **Regel aktivieren**.

     Das Kontrollkästchen **Regel aktivieren** ist standardmäßig aktiviert.

   - Geben Sie im Feld **Tag** den Namen des Tags ein.

     Der Name des Tags darf nicht mehr als 255 Zeichen umfassen und keine Sonderzeiten (wie `"*<>?\:|`) enthalten.

6. Klicken Sie im Abschnitt **Bedingungen** auf die Schaltfläche **Hinzufügen**, um eine neue Bedingung hinzuzufügen, oder klicken Sie auf die Schaltfläche **Eigenschaften**, um eine bestehende Bedingung zu ändern.

   Das Fenster des Assistenten für das Erstellen einer Bedingung der Regel zur automatische Tag-Zuweisung wird geöffnet.

7. Aktivieren Sie im Fenster **Bedingung für die Zuweisung eines Tags** die Kontrollkästchen für jene Bedingungen, die einen Einfluss auf die Zuweisung des Tags haben sollen. Es können mehrere Bedingungen ausgewählt werden.

8. Abhängig von den ausgewählten Bedingungen für die Zuweisung eines Tags zeigt der Assistent Fenster für die Einstellungen der entsprechenden Bedingungen an. Passen Sie das Auslösen der Regel gemäß den folgenden Bedingungen an:

    - **Verwendung oder Netzwerkzugehörigkeit des Geräts** – Netzwerkeigenschaften des Geräts (beispielsweise Gerätename im Windows-Netzwerk und Zugehörigkeit des Geräts zur Domäne oder einem IP-Subnetz).

      Wenn für die Datenbank, die Sie für Kaspersky Security Center verwenden, die Unterscheidung zwischen Groß- und Kleinschreibung festgelegt ist, behalten Sie die Groß- und Kleinbuchstaben bei, wenn Sie einen DNS-Namen für das Gerät angeben. Andernfalls funktioniert Regel der automatischen Tag-Zuweisung nicht.

    - **Verwendung von Active Directory** – Vorhandensein des Gerätes in einer Active Directory-Organisationseinheit und Zugehörigkeit des Gerätes zu einer Active Directory-Gruppe.

    - **Bestimmte Programme** – Vorhandensein des Administrationsagenten auf dem Gerät, Typ, Version und Betriebssystemarchitektur.

    - **Virtuelle Maschinen** – Zugehörigkeit des Geräts zu verschiedenen Typen von virtuellen Maschinen.

    - **Anwendung aus Programm-Registry installiert** – Vorhandensein von Programmen verschiedener Hersteller auf dem Gerät.

9. Geben Sie nach den Einstellungen der Bedingung den Namen der Bedingung ein und schließen Sie den Assistenten ab.

    Falls erforderlich, können mehrere Bedingungen für eine Regel festgelegt werden. In diesem Fall wird den Geräten das Tag zugewiesen, wenn mindestens eine der Bedingungen erfüllt wird. Die hinzugefügten Bedingungen werden im Eigenschaftenfenster der Regel angezeigt.

10. Klicken Sie im Fenster **Neue Regel** auf die Schaltfläche **OK** und anschließend im Eigenschaftenfenster des Administrationsservers nochmals auf **OK**.

Die erstellten Regeln wird auf Geräten ausgeführt, die vom ausgewählten Administrationsserver verwaltet werden. Wenn die Einstellungen für das Gerät den Bedingungen der Regel entsprechen, wird diesem Gerät das Tag zugewiesen.

Anzeige und Einstellungen von Tags, die dem Gerät zugewiesen sind

Sie können eine Liste aller Tags anzeigen, die dem Gerät zugewiesen sind, sowie zu den Einstellungen der Regeln für die automatische Tag-Zuweisung an Geräte im Eigenschaftenfenster des Geräts wechseln.

Um die dem Gerät zugewiesenen Tags anzuzeigen und anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte**.

2. Wählen Sie im Arbeitsbereich des Ordners **Verwaltete Geräte** das Gerät aus, für das Sie die zugewiesenen Tags anzeigen möchten.

3. Wählen Sie im Kontextmenü des gewünschten Geräts den Punkt **Eigenschaften** aus.

4. Wählen Sie im Eigenschaftenfenster des Geräts den Abschnitt **Tags** aus.

   Es wird die Liste der Tags, die dem ausgewählten Gerät zugewiesen sind, sowie die Zuweisungsmethode des Tags angezeigt: manuell oder nach Regel.

5. Führen Sie erforderlichenfalls eine der folgenden Aktionen aus:

   - Um zu den Einstellungen der Regeln zur Zuweisung von Tags zu wechseln, klicken Sie auf den Link **Regeln für die automatische Tag-Zuweisung einrichten** (nur für Windows).
   - Um einen Tag umzubenennen, markieren Sie den Tag und klicken Sie auf die Schaltfläche **Umbenennen**.
   - Um einen Tag zu löschen, markieren Sie den Tag und klicken Sie auf **Löschen**.
   - Um einen Tag manuell hinzuzufügen, geben Sie den Tag im Feld im unteren Bereich des Abschnitts **Tags** ein und klicken Sie auf die Schaltfläche **Hinzufügen**.

6. Klicken Sie auf die Schaltfläche **Übernehmen**, wenn Sie Änderungen im Abschnitt **Tags** gemacht haben, damit Ihre Änderungen in Kraft treten.

7. Klicken Sie auf die Schaltfläche **OK**.

Wenn Sie einen Tag in den Eigenschaften des Geräts gelöscht oder umbenannt haben, erstreckt sich diese Änderung nicht auf die Regeln zur Zuweisung von Tags, die in den Eigenschaften des Administrationsservers festgelegt sind. Die Änderung wird nur auf jenes Gerät angewendet, an dessen Eigenschaften Sie die Änderungen vorgenommen haben.

Ferndiagnose der Client-Geräte. Kaspersky Security Center Ferndiagnosetool

Das Ferndiagnosetool von Kaspersky Security Center (im Folgenden auch Ferndiagnosetool genannt) dient zur Ausführung folgender Operationen auf den Client-Geräten:

- Ablaufverfolgung aktivieren und deaktivieren, Ablaufverfolgungsstufe ändern, Protokolldatei downloaden
- Herunterladen von Systeminformationen und Programmeinstellungen
- Ereignisprotokolle downloaden
- Erzeugen einer Dump-Datei für eine Anwendung
- Diagnose starten und Diagnoseberichte herunterladen
- Programme starten und beenden

Sie können Ereignisprotokolle und Diagnoseberichte verwenden, die von einem Client-Gerät heruntergeladen wurden, um selbst Probleme zu beheben. Außerdem könnte Sie einen Experten des Technischen Supports von Kaspersky auffordern, Protokolldateien, Dump-Dateien, Ereignisprotokolle und Diagnoseberichte von einem Client-Gerät zur weiteren Analyse bei Kaspersky herunterzuladen.

Das Ferndiagnosetool wird automatisch mit der Verwaltungskonsole auf dem Gerät installiert.

Ferndiagnosetool mit dem Client-Gerät verbinden

Um das Ferndiagnosetool mit einem Client-Gerät zu verbinden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur eine beliebige Administrationsgruppe aus.
2. Klicken Sie mit der rechten Maustaste im Arbeitsbereich auf der Registerkarte **Geräte** auf das Kontextmenü eines beliebigen Geräts und wählen **Externe Tools** → **Remote-Diagnose** aus.

   Daraufhin wird das Hauptfenster des Ferndiagnosetools geöffnet.
3. Bestimmen Sie im ersten Feld des Hauptfensters, wie das Tool mit dem Gerät verbunden werden soll:
   - **Zugriff mittels Microsoft Windows Netzwerk**.
   - **Zugriff mittels Administrationsserver**.
4. Bei Auswahl im ersten Feld der Variante **Zugriff mittels Microsoft Windows Netzwerk** gehen Sie wie folgt vor:
   - Geben Sie im Feld **Gerät** die Adresse des Geräts an, mit dem das Tool verbunden werden soll

     Als Geräteadresse kann die IP-Adresse, der NetBIOS-Name oder der DNS-Name angegeben werden.

     In der Standardeinstellung ist die Adresse des Geräts angegeben, aus dessen Kontextmenü das Tool aufgerufen wurde.
   - Geben Sie das Benutzerkonto zur Herstellung der Verbindung mit dem Gerät an:
     - **Im Namen des aktuellen Benutzers verbinden** (Standardmäßig ausgewählt). Stellen Sie unter Verwendung des aktuellen Benutzerkontos eine Verbindung her.
     - **Angegebenen Benutzernamen und Kennwort verwenden**. Stellen Sie unter Verwendung des verfügbaren Benutzerkontos eine Verbindung her. Geben Sie **Benutzername** und **Kennwort** des gewünschten Benutzerkontos an.

     Die Verbindung zum Gerät ist nur unter dem Benutzerkonto des lokalen Administrators des Geräts möglich.
5. Bei Auswahl im ersten Feld der Variante **Zugriff mittels Administrationsserver** gehen Sie wie folgt vor:
   - Geben Sie im Feld **Administrationsserver** die Adresse des Administrationsservers an, über den eine Verbindung mit dem Gerät hergestellt werden soll.

     Als Serveradresse kann die IP-Adresse, der NetBIOS-Name oder der DNS-Name angegeben werden.

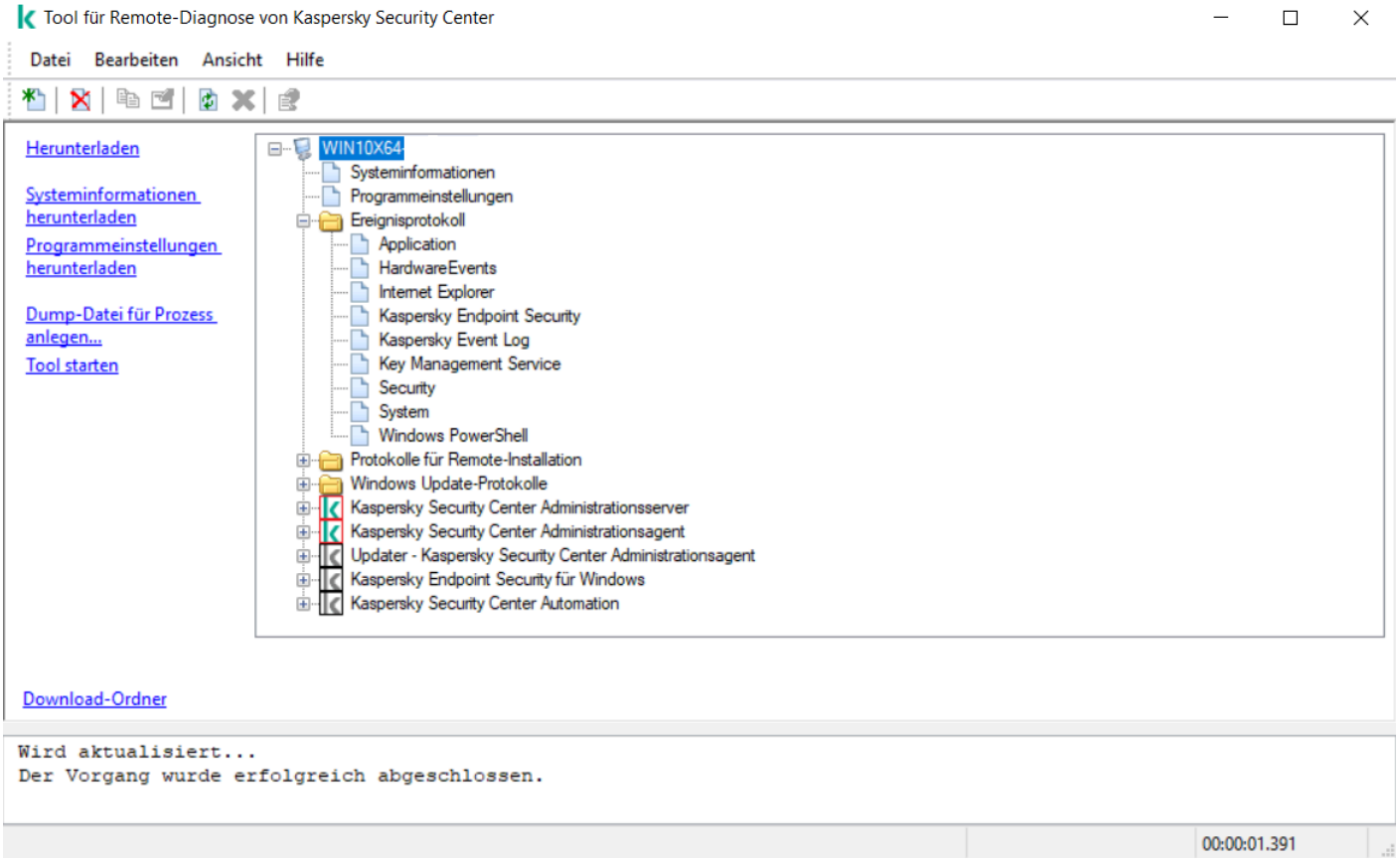
     In der Standardeinstellung ist die Adresse des Administrationsservers angegeben, von dem aus das Tool gestartet wurde.
   - Aktiveren Sie bei Bedarf die Kontrollkästchen **SSL verwenden**, **Daten komprimieren** und **Das Gerät gehört zu sekundärem Administrationsserver**.

     Wenn das Kontrollkästchen **Das Gerät gehört zu sekundärem Administrationsserver** aktiviert ist, können Sie im Feld **Das Gerät gehört zu sekundärem Administrationsserver** einen sekundären Administrationsserver auswählen, der das Gerät verwaltet. Klicken Sie dazu auf **Durchsuchen**.

6. Um eine Verbindung mit dem Gerät herzustellen, klicken Sie auf **Anmelden**.

Wenn für Ihr Konto die zweistufige Überprüfung aktiviert ist, müssen Sie sich mittels zweistufiger Überprüfung autorisieren.

Daraufhin wird das Fenster für Remote-Diagnose des Geräts geöffnet (s. Abb. unten). Im linken Fensterbereich befinden sich die Links für die Ausführung von Vorgängen zur Diagnose des Geräts. Im rechten Fensterbereich wird die Struktur mit den Objekten des Geräts angezeigt, die für das Tool verfügbar sind. Im unteren Fensterbereich wird der Fortschritt der ausgeführten Vorgänge angezeigt.



Tool zur Remote-Diagnose. Fenster zur Remote-Diagnose des Geräts

Das Tool für die Remote-Diagnose speichert die von den Geräten heruntergeladenen Dateien auf dem Desktop des Geräts, von dem aus es gestartet wurde.

Erzeugen einer Dump-Datei für eine Anwendung

Mit einer Dump-Datei für eine Anwendung können Sie die Parameter der Anwendung anzeigen, die an einem bestimmten Zeitpunkt auf einem Client-Gerät ausgeführt wird. Diese Datei enthält auch Informationen über die Module, die für eine Anwendung geladen wurden.

Das Erstellen von Dumps wird für Linux-Geräte nicht unterstützt.

Um Dumps mittels Ferndiagnose zu erstellen, wird das Tool "kldumper" verwendet. Dieses Tool erstellt Prozess-Dumps von Kaspersky-Anwendungen auf Anfrage der Spezialisten des Technischen Supports. Ausführliche Informationen über die Voraussetzungen zur Verwendung des kldumper-Tools finden Sie in der Wissensdatenbank von Kaspersky Security Center.

So erzeugen Sie eine Dump-Datei für eine Anwendung:

1. Öffnen Sie im Arbeitsbereich des Ordners **Verwaltete Geräte** auf der Registerkarte **Geräte** das Kontextmenü des benötigten Geräts und wählen anschließend die Option **Externe Tools → Remote-Diagnose**.

   Das Fenster **Tool für Remote-Diagnose von Kaspersky Security Center** wird geöffnet.

2. Verbinden Sie das Ferndiagnosetool mit dem Client-Gerät.

   Daraufhin wird das Fenster für die Remote-Diagnose des Geräts geöffnet.

3. Klicken Sie im linken Teil des Fensters auf den Link **Dump-Datei für Prozess anlegen**.

4. Geben Sie im Fenster **Erstellen der Dump-Datei für den Prozess** die ausführbare Datei der Anwendung an, für die Sie eine Dump-Datei erstellen möchten.

5. Klicken Sie auf **OK**.

Es wird ein Archiv mit der Dump-Datei für die angegebene Anwendung heruntergeladen.

Wenn die angegebene Anwendung nicht auf dem Client-Gerät ausgeführt wird, ist der Ordner "result" im heruntergeladenen Archiv leer.

Wenn die angegebene Anwendung ausgeführt wird, aber der Download fehlschlägt oder der Ordner "result" im heruntergeladenen Archiv leer ist, schlagen Sie in der Wissensdatenbank von Kaspersky Security Center nach.

Ablaufverfolgung aktivieren und deaktivieren, Protokolldatei downloaden

Um die Ablaufverfolgung auf einem Remote-Gerät zu aktivieren, gehen Sie wie folgt vor:

1. Starten Sie das Tool für die Remote-Diagnose, und stellen Sie eine Verbindung mit dem gewünschten Gerät her.

2. Wählen Sie in der Objektstruktur des Geräts die Anwendung aus, für die Sie die Ablaufverfolgung aktivieren möchten.

   Die Aktivierung und Deaktivierung der Ablaufverfolgung bei Anwendungen mit Selbstschutz ist nur bei der Verbindung mit dem Gerät mittels Administrationsserver möglich.

   Wenn Sie die Ablaufverfolgung für den Administrationsagenten aktivieren möchten, können Sie dies auch tun, während Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen erstellen. Der Administrationsagent erfasst in diesem Fall die Ablaufverfolgungsinformationen, selbst wenn die Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist.

3. Um die Ablaufverfolgung zu aktivieren, gehen Sie wie folgt vor:

   a. Klicken Sie im linken Fensterbereich des Tools zur Remote-Diagnose auf **Ablaufverfolgung aktivieren**.

   b. Wir empfehlen Ihnen, im nächsten Fenster **Ablaufverfolgungsstufe auswählen** die Standardwerte der Einstellungen beizubehalten. Bei Bedarf führt Sie ein Spezialist des Technischen Supports durch den Konfigurationsprozess. Es sind folgende Einstellungen verfügbar:

      - **Ablaufverfolgungsstufe**

        Die Ablaufverfolgungsstufe definiert die Detailstufe der Protokolldatei.

      - **Ablaufverfolgung auf Basis von Rotation** (nur verfügbar für Kaspersky Endpoint Security)

        Die Anwendung überschreibt die Ablaufverfolgungsinformationen, um eine übermäßige Größenzunahme der Protokolldatei zu vermeiden. Geben Sie die maximale Anzahl von Dateien, die zum Speichern der Ablaufverfolgungsdaten verwendet werden sollen sowie die maximale Größe jeder Datei, an. Wenn die maximale Anzahl von Protokolldateien in maximaler Größe erreicht ist, wird die älteste Protokolldatei gelöscht, damit eine neue Protokolldatei erstellt werden kann.

   c. Klicken Sie auf die Schaltfläche **OK**.

4. Für Kaspersky Endpoint Security kann ein Spezialist des Technischen Supports Sie dazu auffordern, die Xperf-Ablaufverfolgung zu aktivieren, um Informationen über die Systemleistung zu erhalten.

   So aktivieren Sie die Xperf-Ablaufverfolgung:

   a. Klicken Sie im linken Fensterbereich des Tools zur Remote-Diagnose auf **Xperf-Ablaufverfolgung aktivieren**.

   b. Wählen Sie im nächsten Fenster **Ablaufverfolgungsstufe auswählen** je nach Anweisung des Spezialisten des technischen Supports eine der folgenden Ablaufverfolgungsstufen aus:

      - **Leichte Stufe**

        Eine Protokolldatei dieses Typs enthält die Mindestmenge an Informationen über das System.

        Diese Variante ist standardmäßig ausgewählt.

      - **Tiefe Stufe**

        Eine Protokolldatei dieses Typs enthält detailliertere Informationen als Protokolldateien vom Typ *Leicht* und kann von den Experten des Technischen Supports angefordert werden, wenn eine Protokolldatei vom Typ *Leicht* nicht für die Beurteilung der Leistung ausreicht. Die Protokolldatei der Stufe *Tief* enthält technische Informationen zum System einschließlich: Informationen zur Hardware und zum Betriebssystem; Liste der gestarteten und abgeschlossenen Prozesse und Anwendungen; Ereignisse, die für die Leistungsbewertung verwendet wurden; Ereignisse aus dem Windows-Systembewertungstool.

   c. Wählen Sie eine der folgenden Ablaufverfolgungstypen aus:

      - **Basistyp**

        Die Ablaufverfolgungsinformationen werden während der Ausführung der Sicherheitsanwendung Kaspersky Endpoint Security empfangen.

        Diese Variante ist standardmäßig ausgewählt.

- **Bei-Neustart-Typ**

  Die Ablaufverfolgungsinformationen werden empfangen, während das Betriebssystem auf dem verwalteten Gerät gestartet wird. Diese Art von Ablaufverfolgung ist wirksam, wenn das Problem, das die Systemleistung beeinträchtigt, nach dem Einschalten des Geräts und vor dem Start von Kaspersky Endpoint Security auftritt.

d. Sie werden möglicherweise auch aufgefordert, die Option **Ablaufverfolgung auf Basis von Rotation** zu aktivieren, um eine übermäßige Größenzunahme der Protokolldateien zu vermeiden. Geben Sie dann die maximale Größe der Protokolldatei an. Wenn die Datei die maximale Größe erreicht, werden die ältesten Informationen der Ablaufverfolgung durch neue Informationen überschrieben.

e. Klicken Sie auf die Schaltfläche **OK**.

In einigen Fällen ist es erforderlich, die Sicherheitsanwendungen und deren Aufgabe neu zu starten, um die Ablaufverfolgung zu aktivieren.

Das Tool zur Remote-Diagnose aktiviert die Ablaufverfolgung für die ausgewählte Anwendung.

Um eine Protokolldatei einer Anwendung herunterzuladen, gehen Sie wie folgt vor:

1. Führen Sie das Tool zur Remote-Diagnose aus und verbinden Sie das gewünschte Gerät wie in Ferndiagnosetool mit dem Client-Gerät verbinden beschrieben.
2. Wählen Sie im Knoten der Anwendung im Ordner **Protokolldateien** die gewünschte Datei aus.
3. Klicken Sie im linken Fensterbereich des Tools zur Remote-Diagnose auf **Vollständige Datei herunterladen**.

   Bei großen Dateien können die aktuellsten Teile der Ablaufverfolgung heruntergeladen werden.

   Sie können die markierte Protokolldatei löschen. Das Löschen der Datei ist jedoch erst nach Deaktivierung der Ablaufverfolgung möglich.

Die ausgewählte Datei wird in den Speicherort heruntergeladen, der im unteren Teil des Fensters angegeben ist.

Um die Ablaufverfolgung auf einem Remote-Gerät zu deaktivieren, gehen Sie wie folgt vor:

1. Führen Sie das Tool zur Remote-Diagnose aus und verbinden Sie das gewünschte Gerät wie in Ferndiagnosetool mit dem Client-Gerät verbinden beschrieben.
2. Wählen Sie in der Objektstruktur des Geräts die Anwendung aus, für die Sie die Ablaufverfolgung deaktivieren möchten.

   Die Aktivierung und Deaktivierung der Ablaufverfolgung bei Anwendungen mit Selbstschutz ist nur bei der Verbindung mit dem Gerät mittels Administrationsserver möglich.

3. Klicken Sie im linken Fensterbereich des Tools zur Remote-Diagnose auf **Ablaufverfolgung deaktivieren**.

Das Tool zur Remote-Diagnose deaktiviert die Ablaufverfolgung für die ausgewählte Anwendung.

Anwendungseinstellungen herunterladen

Um die Programmeinstellungen von einem Remote-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Führen Sie das Tool zur Remote-Diagnose aus und verbinden Sie das gewünschte Gerät wie in Ferndiagnosetool mit dem Client-Gerät verbinden beschrieben.
2. Wählen Sie in der Objektstruktur des Fensters des Tools zur Remote-Diagnose den obersten Knoten mit dem Namen des Geräts aus.
3. Wählen Sie im linken Fensterbereich des Tools zur Remote-Diagnose die erforderliche Aktion aus den folgenden Optionen aus:
   - **Systeminformationen herunterladen**
   - **Programmeinstellungen herunterladen**
   - **Dump-Datei für Prozess anlegen**

     Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie die ausführbare Datei für die Anwendung angeben können, für die Sie eine Dump-Datei anlegen möchten.
   - **Tool starten**

     Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie die ausführbare Datei des Tools und die Einstellungen für dessen Start angeben können.

Daraufhin wird das gewählte Tool auf dem Gerät heruntergeladen und gestartet.

Ereignisprotokolle downloaden

Um das Ereignisprotokoll von einem Remote-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Führen Sie das Tool zur Remote-Diagnose aus und verbinden Sie das gewünschte Gerät wie in Ferndiagnosetool mit dem Client-Gerät verbinden beschrieben.
2. Wählen Sie im Ordner **System-Ereignisprotokolle** der Objektstruktur des Geräts das gewünschte Protokoll aus.
3. Laden Sie das ausgewählte Protokoll herunter, indem Sie auf den Link **Ereignisprotokoll <Name des Ereignisprotokolls> downloaden** im linken Fensterbereich des Tools zur Remote-Diagnose klicken.

Das ausgewählte Ereignisprotokoll wird in den im unteren Bereich angegebenen Ort heruntergeladen.

Herunterladen mehrerer Diagnoseinformationselemente

Das Tool zur Remote-Diagnose von Kaspersky Security Center erlaubt Ihnen, mehrere Elemente von Diagnoseinformationen wie Ereignisprotokolle, Systeminformationen, Protokolldateien und Dump-Dateien herunterzuladen.

Um Diagnoseinformationen von einem Remote-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Führen Sie das Tool zur Remote-Diagnose aus und verbinden Sie das gewünschte Gerät wie in Ferndiagnosetool mit dem Client-Gerät verbinden beschrieben.
2. Klicken Sie im linken Fensterbereich des Tools zur Remote-Diagnose auf **Herunterladen**.
3. Aktivieren Sie die Kontrollkästchen neben den Elementen, die Sie herunterladen möchten.
4. Klicken Sie auf die Schaltfläche **Starten**.

Jedes ausgewählte Element wird in den im unteren Bereich angegebenen Ort heruntergeladen.

Diagnose starten und die Ergebnisse herunterladen

Um die Diagnose für ein Programm auf einem Remote-Gerät zu starten und die Ergebnisse herunterzuladen, gehen Sie wie folgt vor:

1. Führen Sie das Tool zur Remote-Diagnose aus und verbinden Sie das gewünschte Gerät wie in Ferndiagnosetool mit dem Client-Gerät verbinden beschrieben.
2. Wählen Sie in der Objektstruktur des Geräts die gewünschte Anwendung aus.
3. Starten Sie die Diagnose, indem Sie im linken Fensterbereich des Tools zur Remote-Diagnose auf den Link **Diagnose ausführen** klicken.

   Daraufhin wird im Knoten der ausgewählten Anwendung in der Objektstruktur der Diagnosebericht angezeigt.
4. Wählen Sie den erstellten Diagnosebericht in der Objektstruktur aus und klicken Sie auf den Link **Download-Ordner**, um den Bericht herunterzuladen.

Der ausgewählte Bericht wird in den im unteren Bereich angegebenen Ort heruntergeladen.

Starten, Beenden und Neustart von Programmen

Starten, Beenden und Neustart der Programme sind nur bei der Verbindung mit dem Gerät mittels Administrationsserver möglich.

Um eine Anwendung zu starten, zu beenden oder neu zu starten, gehen Sie wie folgt vor:

1. Führen Sie das Tool zur Remote-Diagnose aus und verbinden Sie das gewünschte Gerät wie in Ferndiagnosetool mit dem Client-Gerät verbinden beschrieben.
2. Wählen Sie in der Objektstruktur des Geräts die gewünschte Anwendung aus.

3. Wählen Sie eine Aktion im linken Fensterbereich des Tools zur Remote-Diagnose aus:

   - **Programm beenden**
   - **Programm neu starten**
   - **Programm starten**

   Je nach ausgewählter Aktion wird die Anwendung gestartet, beendet oder neu gestartet.

UEFI-Schutzgeräte

Ein *Gerät mit Schutz auf UEFI-Ebene* ist ein Gerät mit einer Lösung oder Anwendung von Kaspersky, die auf BIOS-Ebene integriert ist. Der integrierte Schutz gewährleistet die Sicherheit des Geräts bereits ab Beginn des Systemstarts, während der Schutz für Geräte, die keine integrierte Software haben, erst nach dem Start der Sicherheitsanwendung in Aktion tritt. Kaspersky Security Center unterstützt die Verwaltung von solchen Geräten.

Um die Einstellungen der Verbindung von Geräten mit Schutz auf UEFI-Ebene zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Verbindungseinstellungen des Servers → Zusätzliche Ports** aus.
4. Ändern Sie im Abschnitt **Zusätzliche Ports** die gewünschten Einstellungen:

   - **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS öffnen**

     Geräte mit Schutz auf UEFI-Ebene können eine Verbindung mit dem Administrationsserver herstellen.

   - **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS**

     Sie können die Portnummer ändern, wenn die Option **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS öffnen** aktiviert ist. Standardmäßig wird Portnummer 13294 verwendet.

5. Klicken Sie auf die Schaltfläche **OK**.

Einstellungen eines verwalteten Geräts

Um die Einstellungen eines verwalteten Geräts anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
2. Wählen Sie im Arbeitsbereich des Ordners ein Gerät aus.
3. Wählen Sie im Kontextmenü des Geräts den Punkt **Eigenschaften** aus.

Das Eigenschaftenfenster des ausgewählten Geräts wird geöffnet; der Abschnitt **Allgemein** ist ausgewählt.

Allgemein

Der Abschnitt **Allgemein** enthält allgemeine Informationen über das Client-Gerät. Die Informationen beruhen auf Daten, die bei der letzten Synchronisierung des Client-Geräts mit dem Administrationsserver empfangen wurden:

- **Name**

  In diesem Feld steht der Name des Client-Geräts in der Administrationsgruppe und der Name kann geändert werden.

- **Beschreibung**

  In diesem Feld können Sie eine zusätzliche Beschreibung für das Client-Gerät eingeben.

- **Windows-Domäne**

  Windows-Domäne oder Arbeitsgruppe, zu der das Gerät gehört.

- **NetBIOS-Name**

  Name des Client-Geräts im Windows-Netzwerk.

- **DNS-Name**

  Name der DNS-Domäne des Client-Geräts.

- **IP-Adresse**

  IP-Adresse des Geräts.

- **Gruppe**

  Administrationsgruppe, zu der das Client-Gerät gehört.

- **Zuletzt aktualisiert**

  Datum des letzten Updates der Antiviren-Datenbanken oder der Programme auf dem Gerät.

- **Zuletzt im Netzwerk sichtbar**

  Zeitpunkt (Datum und Uhrzeit), zu dem das Gerät zuletzt im Netzwerk gesehen wurde.

- **Verbindung mit dem Administrationsserver**

  Datum und Uhrzeit der letzten Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver.

- **Verbindung mit Administrationsserver nicht trennen**

  Wenn diese Option aktiviert ist, wird die dauerhafte Verbindung zwischen dem verwalteten Gerät und dem Administrationsserver aufrecht erhalten. Sie können diese Option verwenden, wenn Sie keine Push-Server einsetzen, die eine solche Verbindung bereitstellen.

  Wenn diese Option deaktiviert ist und keine Push-Server verwendet werden, verbindet sich das verwaltete Gerät nur zur Datensynchronisierung oder Datenübertragung mit dem Administrationsserver.

  Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

Diese Option ist auf verwalteten Geräten standardmäßig deaktiviert. Diese Option ist auf dem Gerät, auf dem der Administrationsserver installiert ist, standardmäßig aktiviert und bleibt selbst dann aktiviert, wenn Sie versuchen, sie zu deaktivieren.

Schutz

Im Abschnitt **Schutz** werden Informationen über den Status des Antiviren-Schutzes auf dem Client-Gerät angezeigt:

- **Gerätestatus**

  Status des Client-Geräts, der ihm anhand der vom Administrator festgelegten Kriterien den Status des Antiviren-Schutzes und der Aktivität des Geräts im Netzwerk zugewiesen wird.

- **Alle Probleme**

  Diese Tabelle enthält eine vollständige Liste mit Problemen, die von den verwalteten Anwendungen gefunden wurden, die auf dem Client-Gerät installiert sind. Jedes Problem wird von einem Status begleitet, den die Anwendung für dieses Problem vorschlägt, dem Gerät zuzuweisen.

- **Echtzeitschutz**

  Dieses Feld zeigt den aktuellen Status des Echtzeitschutzes auf dem Client-Gerät an.

  Wenn sich der Status auf dem Gerät ändert, wird der neue Status erst im Eigenschaftenfenster des Geräts angezeigt, nachdem das Client-Gerät mit dem Administrationsserver synchronisiert wurde.

- **Letzte Untersuchung auf Befehl**

  Datum und Uhrzeit der letzten Schadsoftware-Untersuchung auf einem Client-Gerät.

- **Gesamtzahl der gefundenen Bedrohungen**

  Gesamtzahl der auf einem Client-Gerät gefundenen Bedrohungen seit der Installation der Sicherheitsanwendung (seit der ersten Untersuchung des Geräts) oder seit dem letzten Zurücksetzen des Zählers.

- **Aktive Bedrohungen**

  Anzahl der unverarbeiteten Dateien auf einem Client-Gerät.

  In diesem Feld wird die Anzahl der unverarbeiteten Dateien auf mobilen Geräten nicht berücksichtigt.

- **Status der Datenträgerverschlüsselung**

  Aktueller Status der Verschlüsselung von Dateien auf den lokalen Laufwerken des Geräts. Eine Beschreibung der Statuswerte finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Programme

Im Abschnitt **Programme** wird eine Liste der Kaspersky-Anwendungen angezeigt, die auf dem Client-Gerät installiert sind. Dieser Abschnitt enthält die Schaltflächen zum Starten () und Stoppen (), erforderlicher Kaspersky-Anwendungen (mit Ausnahme des Administrationsagenten). Diese Schaltflächen sind aktiv, wenn auf dem verwalteten Gerät der UDP-Port 15000 für den Empfang von Push-Benachrichtigungen vom Administrationsserver verfügbar ist. Wenn das verwaltete Gerät nicht für Push-Benachrichtigungen verfügbar ist, aber der Modus für die dauerhafte Verbindung mit dem Administrationsserver aktiviert ist (d. h., im Abschnitt **Allgemein** ist die Option **Verbindung mit Administrationsserver nicht trennen** aktiviert), stehen auch die Schaltflächen zum Starten und Stoppen zur Verfügung. Außerdem enthält der Abschnitt **Programme** die folgenden Schaltflächen:

- **Ereignisse**

  Durch Klicken auf diese Schaltfläche können Sie eine Liste der Ereignisse, die bei der Ausführung des Programms auf den Client-Geräten eintreten, sowie die Ergebnisse der Aufgabenausführung für dieses Programm anzeigen lassen.

- **Statistik**

  Durch Klicken auf diese Schaltfläche werden aktuelle Statistikdaten über die Ausführung des Programms angezeigt.

- **Eigenschaften**

  Durch Klicken auf diese Schaltfläche können Sie sich Informationen über das Programm anzeigen lassen und die Programmeinstellungen anpassen.

Aufgaben

In der Registerkarte **Aufgaben** können Sie die Aufgaben eines Client-Geräts verwalten: Liste der vorhandenen Aufgaben anzeigen, neue Aufgaben erstellen, Aufgaben entfernen, starten und beenden, Aufgabeneinstellungen ändern und die Ergebnisse der Aufgabenausführung anzeigen. Die Aufgabenliste beruht auf Daten, die während der letzten Synchronisierung des Clients mit dem Administrationsserver empfangen wurden. Die Daten über den Aufgabenstatus erhält der Administrationsserver vom Client-Gerät.

Diese Schaltflächen zum Starten (), Stoppen () und Löschen () sind aktiv, wenn auf dem verwalteten Gerät der UDP-Port 15000 für den Empfang von Push-Benachrichtigungen vom Administrationsserver verfügbar ist. Wenn das verwaltete Gerät nicht für Push-Benachrichtigungen verfügbar ist, aber der Modus für die dauerhafte Verbindung mit dem Administrationsserver aktiviert ist (d. h., im Abschnitt **Verbindung mit Administrationsserver nicht trennen** ist die Option **Allgemein** aktiviert), stehen auch die Schaltflächen zum Starten, Stoppen und Löschen zur Verfügung.

Wenn keine Verbindung besteht, wird kein Aufgabenstatus angezeigt und die Schaltflächen sind nicht verfügbar.

Ereignisse

Die Registerkarte **Ereignisse** enthält die Ereignisse, die für das ausgewählte Client-Gerät auf dem Administrationsserver registriert wurden.

Sie können die Ereignisse von Geräten exportieren, kopieren und löschen.

Tags

In der Registerkarte **Tags** können Sie die Liste der Schlüsselwörter verwalten, auf deren Grundlage die Suche nach Client-Geräten ausgeführt wird: Liste der vorhandenen Tags anzeigen, Tags aus der Liste zuweisen, Regeln für die automatische Zuweisung von Tags konfigurieren, neue Tags hinzufügen und alte Tags umbenennen, sowie Tags löschen.

Systeminformationen

Im Abschnitt **Allgemeine Systeminformationen** werden Daten zum Programm angezeigt, das auf dem Client-Gerät installiert ist.

Programm-Registry

In Abschnitt **Programm-Registry** können Sie die Registry der auf dem Client-Gerät installierten Programme und der Programm-Updates anzeigen lassen und die Darstellung der Programm-Registry konfigurieren.

Die Daten über die installierten Programme sind verfügbar, wenn der auf dem Client-Gerät installierte Administrationsagent die erforderlichen Daten auf den Administrationsserver überträgt. Die Einstellungen für die Übertragung der Informationen an den Administrationsserver können Sie im Eigenschaftenfenster des Administrationsagenten oder seiner Richtlinie im Abschnitt **Datenverwaltung** anpassen.

- **Nur inkompatible Sicherheitsanwendungen anzeigen**

  Wenn Sie diese Option aktivieren, werden in der Programmliste nur die Sicherheitsanwendungen angezeigt, die nicht mit Kaspersky-Anwendungen kompatibel sind.

  Diese Option ist standardmäßig deaktiviert.

- **Updates anzeigen**

  Wenn Sie diese Option aktivieren, werden in der Programmliste nicht nur Programme, sondern auch die für die Programme installierten Update-Pakete angezeigt.

  Um die Liste der Updates anzuzeigen, werden 100 KB an Datenverkehr benötigt. Wenn Sie die Liste schließen und wieder öffnen, fallen erneut 100 KB an Datenverkehr an.

  Diese Option ist standardmäßig deaktiviert.

- **In Datei exportieren**

  Klicken Sie auf diese Schaltfläche, um die Liste der Programme, die auf dem Gerät installiert sind, als csv- oder txt-Datei zu exportieren.

- **Verlauf**

  Klicken Sie auf diese Schaltfläche, um Ereignisse anzuzeigen, die sich auf die Installation von Programmen auf dem Gerät beziehen. Folgende Informationen werden angezeigt:

  - Datum und Uhrzeit der Installation des Programms auf dem Gerät
  - Name der Anwendung
  - Anwendungsversion

- **Eigenschaften**

  Klicken Sie auf diese Schaltfläche, um die Eigenschaften des Programms anzuzeigen, das in der Liste der auf dem Gerät installierten Programme ausgewählt wurde. Folgende Informationen werden angezeigt:

  - Name der Anwendung
  - Anwendungsversion
  - Programmhersteller

Ausführbare Dateien

In Abschnitt **Ausführbare Dateien** werden ausführbare Dateien angezeigt, die auf dem Client-Gerät entdeckt wurden.

Hardware-Register

Im Abschnitt **Hardware-Register** finden Sie Informationen zur Hardware, die auf dem Client-Gerät installiert ist. Diese Informationen können Sie für Windows-Geräte und Linux-Geräte anzeigen.

Stellen Sie sicher, dass auf den Linux-Geräten, von denen Sie die Hardware-Details abrufen möchten, das Tool lshw installiert ist. Die von virtuellen Maschinen abgerufenen Hardwaredetails können je nach verwendetem Hypervisor unvollständig sein.

Wenn der Administrationsagent auf einem Windows-Gerät installiert ist, sendet er nur die folgenden Informationen über die Gerätehardware an den Administrationsserver:

- Arbeitsspeicher
- Massenspeichergeräte
- Mainboard
- Prozessor
- Netzwerkadapter
- Monitore
- Grafikkarte
- Soundkarte

Wenn der Administrationsagent auf einem Linux- oder macOS-Gerät installiert ist, sendet er die folgenden Informationen über die Gerätehardware an den Administrationsserver (vorausgesetzt, diese Information wird durch das Betriebssystem bereitgestellt):

- Gesamtgröße des Arbeitsspeichers
- Gesamtgröße der Massenspeicher
- Mainboard

- Prozessor
- Netzwerkadapter

Sitzungen

Der Abschnitt **Sitzungen** wird nur für Windows-Geräte angezeigt und enthält Informationen über den Besitzer des Client-Geräts sowie über die Benutzerkonten, die auf dem ausgewählten Gerät verwendet wurden.

Die Daten über die Domänenbenutzer werden auf Grundlage der Daten des Active Directory erzeugt. Informationen zu den lokalen Benutzern werden von der auf dem Client-Gerät installierten Windows-Sicherheitskontenverwaltung (Windows Security Account Manager) bereitgestellt.

- **Gerätebesitzer**

  Im Feld **Gerätebesitzer** wird der Name des Benutzers angezeigt, an den sich der Administrator wenden kann, wenn bestimmte Arbeiten am Client-Gerät durchgeführt werden müssen.

  Mithilfe der Schaltflächen **Zuweisen** und **Eigenschaften** können der Gerätebesitzer ausgewählt und Informationen über den als Gerätebesitzer festgelegten Benutzer angezeigt werden.

  Mithilfe der Schaltfläche mit dem roten Kreuz kann der aktuelle Gerätebesitzer gelöscht werden.

Die Liste enthält Konten der Benutzer, die mit dem Client-Gerät arbeiten.

- **Name**

  Name des Geräts im Windows-Netzwerk.

- **Teilnehmername**

  Name des Benutzers (Domänenname oder lokaler Name), der sich mit diesem Gerät im System angemeldet hat.

- **Benutzerkonto**

  Konto des Benutzers, der sich mit diesem Gerät im System angemeldet hat.

- **E-Mail**

  E-Mail-Adresse des Benutzers.

- **Telefon**

  Telefonnummer des Benutzers.

Sicherheitsprobleme

Auf der Registerkarte **Sicherheitsprobleme** können Sie Sicherheitsvorfälle für ein Client-Gerät anzeigen, bearbeiten oder erstellen. Sicherheitsvorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten verwalteten Kaspersky-Anwendungen als auch manuell vom Administrator erstellt werden. Wenn beispielsweise einige Benutzer immer wieder Schadsoftware von Wechseldatenträgern auf Geräte übertragen, kann der Administrator einen Sicherheitsvorfall erstellen. Der Administrator kann im Text des Sicherheitsvorfalls eine kurze Beschreibung des Falls bereitstellen und Aktionen vorschlagen (etwa Disziplinarmaßnahmen gegen einen Benutzer) und einen Link zum Benutzer oder zu den Benutzern hinzufügen.

Ein Vorfall, für den alle erforderlichen Aktionen ausgeführt worden sind, wird als *Bearbeitet* bezeichnet. Das Vorhandensein von nicht bearbeiteten Sicherheitsvorfällen kann als Bedingung für eine Statusänderung des Geräts in *Kritisch* oder *Warnung* ausgewählt werden.

Dieser Abschnitt enthält eine Liste der für das Gerät erstellten Sicherheitsvorfälle. Die Sicherheitsvorfälle werden nach Signifikanz und Art eingestuft. Die Art des Sicherheitsvorfalls wird von der Kaspersky-Anwendung bestimmt, die den Vorfall erstellt hat. Bearbeitete Sicherheitsvorfälle können in der Liste durch Aktivieren des Kontrollkästchens in der Spalte **Bearbeitet** gekennzeichnet werden.

Schwachstellen in Programmen

Im Abschnitt **Schwachstellen in Programmen** können Sie sich Informationen über die Schwachstellen von Drittanbietersoftware anzeigen lassen, die auf den Client-Geräten installiert ist. Mithilfe der Suchzeile oberhalb der Liste können Sie nach Namen nach Schwachstellen suchen.

- **In Datei exportieren**

  Durch Klicken auf die Schaltfläche **In Datei exportieren** können Sie die Schwachstellenliste in einer Datei speichern. Standardmäßig exportiert das Programm die Schwachstellenliste in eine CSV-Datei.

- **Nur Schwachstellen anzeigen, die geschlossen werden können**

  Ist diese Option aktiviert, werden in diesem Abschnitt jene Schwachstellen angezeigt, die durch einen Patch geschlossen werden können.

  Ist diese Option deaktiviert, werden in diesem Abschnitt sowohl Schwachstellen angezeigt, die durch einen Patch geschlossen werden können, als auch Schwachstellen, für die kein Patch vorhanden ist.

  Diese Option ist standardmäßig aktiviert.

- **Eigenschaften**

  Wählen Sie in der Liste eine Software-Schwachstelle aus und klicken Sie auf **Eigenschaften**, um die Eigenschaften der ausgewählten Software-Schwachstelle in einem separaten Fenster anzuzeigen. In dem Fenster können Sie Folgendes tun:

  - Schwachstellen in Programmen auf diesem verwalteten Gerät ignorieren (in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console).
  - Liste mit Korrekturen anzeigen, die für die Schwachstelle empfohlen werden.
  - Programm-Updates manuell angeben, um eine Schwachstelle zu beheben (in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console).
  - Schwachstellen-Instanzen anzeigen.
  - Liste der vorhandenen Aufgaben zur Schwachstellen-Behebung anzeigen, und neue Aufgaben zur Schwachstellen-Behebung erstellen.

Verfügbare Updates

In diesem Abschnitt können Sie sich die Liste der auf dem Gerät gefundenen Software-Updates anzeigen lassen, die nicht installiert wurden. Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Installierte Updates anzeigen**

  Ist diese Option aktiviert, werden in der Update-Liste nicht installierte Updates sowie Updates angezeigt, die auf dem Client-Gerät bereits installiert wurden.

  Diese Option ist standardmäßig deaktiviert.

Aktive Richtlinien

In diesem Abschnitt wird eine Liste mit den Richtlinien für Kaspersky-Anwendungen angezeigt, die diesem Gerät momentan zugewiesen sind.

- **In Datei exportieren**

  Mithilfe der Schaltfläche **In Datei exportieren** können Sie die Liste der aktiven Richtlinien in einer Datei speichern. Standardmäßig exportiert das Programm die Liste der Richtlinien in eine CSV-Datei.

Aktive Richtlinienprofile

- **Aktive Richtlinienprofile**

  In dieser Liste können Informationen über die auf den Client-Geräten aktiven Richtlinienprofile angezeigt werden. Mithilfe der Suchzeile über der Liste können Sie in der Liste aktive Richtlinienprofile nach dem Namen der Richtlinie bzw. Namen des Richtlinienprofils suchen.

- **In Datei exportieren**

  Mithilfe der Schaltfläche **In Datei exportieren** können Sie die Liste der aktiven Richtlinienprofile in einer Datei speichern. Standardmäßig exportiert das Programm die Liste der Richtlinienprofile in eine CSV-Datei.

Verteilungspunkte

In diesem Abschnitt finden Sie eine Liste der Verteilungspunkte, mit denen das Gerät interagiert.

- **In Datei exportieren**

  Mithilfe der Schaltfläche **In Datei exportieren** können Sie die Liste der Verteilungspunkte, mit denen das Gerät interagiert, in einer Datei speichern. Standardmäßig exportiert die Anwendung die Liste der Geräte in eine Datei im csv-Format.

- **Eigenschaften**

  Mithilfe der Schaltfläche **Eigenschaften** können Sie die Einstellungen der Verteilungspunkte, mit denen das Gerät interagiert, anzeigen und anpassen.

Allgemeine Richtlinieneinstellungen

Allgemein

Im Abschnitt **Allgemein** können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:

  - **Aktive Richtlinie**

    Bei Auswahl dieser Option wird die Richtlinie aktiv.

    Diese Variante ist standardmäßig ausgewählt.

  - **Richtlinie für mobile Benutzer**

    Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

  - **Inaktive Richtlinie**

    Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.

- In der Einstellungsgruppe **Einstellungen erben** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:

  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.

  - **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:

    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.

    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

    Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Im Abschnitt **Konfiguration von Ereignissen** können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Die Ereignisse werden anhand der Ereigniskategorie auf folgende Registerkarten aufgeteilt:

- **Kritisch**

  Die Registerkarte **Kritisch** wird in den Eigenschaften der Richtlinie des Administrationsagenten nicht angezeigt.

- **Funktionsfehler**
- **Warnung**
- **Information**

Jede Registerkarte enthält eine Liste mit Ereignistypen und der Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen). Über die Schaltfläche **Eigenschaften** können die Eigenschaften für die Protokollierung und die Benachrichtigung über die aus der Liste ausgewählten Ereignisse festgelegt werden. Standardmäßig werden die allgemeinen Benachrichtigungseinstellungen, die für den gesamten Administrationsserver festgelegt wurden, für alle Ereignistypen verwendet. Bestimmte Einstellungen können jedoch für die gewünschten Ereignistypen angepasst werden.

Sie können beispielsweise auf der Registerkarte **Warnung** den Ereignistyp **Es ist ein Sicherheitsproblem aufgetreten** konfigurieren. Solche Ereignisse können beispielsweise eintreten, wenn der freie Speicherplatz eines Verteilungspunkts weniger als 2 GB beträgt (es sind mindestens 4 GB erforderlich, um Programme remote zu installieren und Updates herunterzuladen). Um das Ereignis **Es ist ein Sicherheitsproblem aufgetreten** zu konfigurieren, wählen Sie es aus und klicken Sie auf die Schaltfläche **Eigenschaften**. Danach können Sie angeben, wo die aufgetretenen Ereignisse gespeichert werden sollen und wie die Benachrichtigung darüber stattfinden soll.

Wenn der Administrationsagent einen Sicherheitsvorfall entdeckt hat, können Sie diesen Vorfall mithilfe der Einstellungen eines verwalteten Geräts verwalten.

Für die Auswahl mehrerer Ereignistypen verwenden Sie die Tasten **Umschalt** oder **Strg**, und für die Auswahl aller Typen verwenden Sie die Schaltfläche **Alle auswählen**.

Richtlinieneinstellungen des Administrationsagenten

Gehen Sie folgendermaßen vor, um die Richtlinieneinstellungen des Administrationsagenten anzupassen:

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Wählen Sie im Arbeitsbereich des Ordners die Richtlinie des Administrationsagenten aus.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Eigenschaften** aus.

Das Eigenschaftenfenster der Richtlinie des Administrationsagenten wird geöffnet.

Der Vergleichstabelle können Sie im Detail entnehmen, wie die folgenden Einstellungen je nach verwendetem Betriebssystemtyp angewendet werden.

Allgemein

Im Abschnitt **Allgemein** können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:

  - **Aktive Richtlinie**

    Bei Auswahl dieser Option wird die Richtlinie aktiv.

    Diese Variante ist standardmäßig ausgewählt.

  - **Richtlinie für mobile Benutzer**

    Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

  - **Inaktive Richtlinie**

    Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.

- In der Einstellungsgruppe **Einstellungen erben** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:

  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.

  - **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:

    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.

    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

    Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Im Abschnitt **Konfiguration von Ereignissen** können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Die Ereignisse werden anhand der Ereigniskategorie auf folgende Registerkarten aufgeteilt:

- **Kritisch**

  Die Registerkarte **Kritisch** wird in den Eigenschaften der Richtlinie des Administrationsagenten nicht angezeigt.

- **Funktionsfehler**
- **Warnung**
- **Information**

Jede Registerkarte enthält eine Liste mit Ereignistypen und der Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen). Über die Schaltfläche **Eigenschaften** können die Eigenschaften für die Protokollierung und die Benachrichtigung über die aus der Liste ausgewählten Ereignisse festgelegt werden. Standardmäßig werden die allgemeinen Benachrichtigungseinstellungen, die für den gesamten Administrationsserver festgelegt wurden, für alle Ereignistypen verwendet. Bestimmte Einstellungen können jedoch für die gewünschten Ereignistypen angepasst werden.

Sie können beispielsweise auf der Registerkarte **Warnung** den Ereignistyp **Es ist ein Sicherheitsproblem aufgetreten** konfigurieren. Solche Ereignisse können beispielsweise eintreten, wenn der freie Speicherplatz eines Verteilungspunkts weniger als 2 GB beträgt (es sind mindestens 4 GB erforderlich, um Programme remote zu installieren und Updates herunterzuladen). Um das Ereignis **Es ist ein Sicherheitsproblem aufgetreten** zu konfigurieren, wählen Sie es aus und klicken Sie auf die Schaltfläche **Eigenschaften**. Danach können Sie angeben, wo die aufgetretenen Ereignisse gespeichert werden sollen und wie die Benachrichtigung darüber stattfinden soll.

Wenn der Administrationsagent einen Sicherheitsvorfall entdeckt hat, können Sie diesen Vorfall mithilfe der Einstellungen eines verwalteten Geräts verwalten.

Für die Auswahl mehrerer Ereignistypen verwenden Sie die Tasten **Umschalt** oder **Strg**, und für die Auswahl aller Typen verwenden Sie die Schaltfläche **Alle auswählen**.

Einstellungen

Im Abschnitt **Einstellungen** können Sie die Richtlinieneinstellungen des Administrationsagenten anpassen:

- **Dateien nur über Verteilungspunkte übertragen**

  Wenn diese Option aktiviert ist, beziehen die Administrationsagenten auf verwalteten Geräten die Updates ausschließlich von Verteilungspunkten.

  Wenn diese Option deaktiviert ist, beziehen die Administrationsagenten auf verwalteten Geräten die Updates von Verteilungspunkten oder vom Administrationsserver.

  > Beachten Sie, dass die Sicherheitsanwendungen auf verwalteten Geräten die Updates aus der Quelle abrufen, die in der Update-Aufgabe für jede Sicherheitsanwendung festgelegt wurde. Wenn Sie die Option **Dateien nur über Verteilungspunkte übertragen** aktivieren, stellen Sie sicher, dass Kaspersky Security Center in den Update-Aufgaben als Update-Quelle festgelegt ist.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Ereigniswarteschlange (MB)**

  In diesem Feld können Sie den maximalen Speicherplatz eingeben, welchen die Ereigniswarteschlange auf dem Laufwerk einnehmen kann.

  Standardmäßig ist der Wert auf 2 MB eingestellt.

- **Dem Programm ist es erlaubt, auf dem Gerät erweiterte Daten über Richtlinien zu erfassen**

  Der Administrationsagent, der auf einem verwalteten Gerät installiert ist, überträgt Informationen über die angewendete Sicherheitsanwendungs-Richtlinie an die Sicherheitsanwendung (z. B. Kaspersky Endpoint Security für Windows). Die übertragenen Informationen können Sie auf der Benutzeroberfläche der Sicherheitsanwendung einsehen.

  Der Administrationsagent überträgt die folgenden Informationen:

  - Zeit, zu der die Richtlinie dem verwalteten Gerät zugestellt wurde.
  - Name der aktiven Richtlinie zum Zeitpunkt der Übertragung der Richtlinien an das verwaltete Gerät.
  - Name der Richtlinie für mobile Benutzer zum Zeitpunkt der Übertragung der Richtlinie an das verwaltete Gerät. (für den Administrationsagenten für Linux nicht verfügbar).
  - Name und vollständiger Pfad der Administrationsgruppe, zu der das verwaltete Gerät gehörte, als die Richtlinie an das verwaltete Gerät zugestellt wurde.
  - Liste der aktiven Richtlinienprofile mit ihren Namen und Prioritäten zum Zeitpunkt der Übertragung der Richtlinien an das verwaltete Gerät.

  Sie können diese Informationen verwenden, um sicherzustellen, dass für das Gerät die richtige Richtlinie verwendet wird, und um Probleme zu lösen. Diese Option ist standardmäßig deaktiviert.

- **Dienst des Administrationsagenten vor unberechtigter Deinstallation und Beendigung schützen sowie Änderung der Einstellungen verhindern**

  Wenn diese Option aktiviert ist, kann nach der Installation des Administrationsagenten auf einem verwalteten Gerät die Komponente nicht ohne die entsprechenden Berechtigungen entfernt oder neu konfiguriert werden. Der Dienst des Administrationsagenten kann nicht beendet werden. Diese Option hat keine Auswirkung auf Domänencontroller.

  Aktivieren Sie diese Option, um den Administrationsagenten auf Workstations zu schützen, die mit lokalen Administratorrechten betrieben werden.

  Diese Option ist standardmäßig deaktiviert.

- **Deinstallationskennwort verwenden**

  Wenn diese Option aktiviert ist, können Sie das Kennwort für das Tool "klmover" und für die Aufgabe zur Remote-Deinstallation des Administrationsagenten angeben. Klicken Sie dazu auf die Schaltfläche **Ändern**.

  Diese Option ist standardmäßig deaktiviert.

Datenverwaltung

Im Abschnitt **Datenverwaltung** können Sie die Objekttypen auswählen, deren Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen.

- **Informationen über Windows-Updates**

  Wenn diese Option aktiviert ist, werden auf den Administrationsserver Informationen über Microsoft Windows-Updates übertragen, die auf den Client-Geräten installiert werden sollen.

  Selbst wenn die Option deaktiviert ist, werden Aktualisierungen manchmal in den Geräteeigenschaften im Abschnitt **Verfügbare Updates** angezeigt. Dies kann beispielsweise vorkommen, wenn die Geräte der Organisation Schwachstellen aufweisen, die durch diese Updates behoben werden können.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Informationen zu Schwachstellen in Programmen und entsprechenden Updates**

  Wenn diese Option aktiviert ist, werden Informationen über Schwachstellen in Drittanbieter-Programmen (Software von Microsoft eingeschlossen), die auf verwalteten Geräten erkannt wurden, sowie Informationen über Programm-Updates zum Beheben der Drittanbieter-Schwachstellen (Software von Microsoft ausgeschlossen) an den Administrationsserver gesendet.

  Das Aktivieren der Option (**Informationen zu Schwachstellen in Programmen und entsprechenden Updates**) erhöht die Netzwerkbelastung, den Speicherbedarf des Administrationsservers und den Ressourcenverbrauch des Administrationsagenten.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

  Um Updates für Software von Microsoft zu verwalten, verwenden Sie die Option **Informationen über Windows-Updates**.

- **Informationen über die Hardware-Inventur**

  Der auf einem Gerät installierte Administrationsagent sendet Informationen über die Geräte-Hardware an den Administrationsserver. Sie können die Hardware-Details in den Geräteeigenschaften anzeigen.

  Stellen Sie sicher, dass das Tool "lshw" auf den Linux-Geräten installiert ist, von denen Sie die Hardwaredetails abrufen möchten. Die von virtuellen Maschinen abgerufenen Hardwaredetails können je nach verwendetem Hypervisor unvollständig sein.

- **Details zu installierten Programmen**

  Ist diese Option aktiviert, werden auf den Administrationsserver Informationen über die auf den Client-Geräten installierten Anwendungen übertragen.

  Diese Option ist standardmäßig aktiviert.

- **Informationen über Patches einbinden**

  Informationen über die auf den Client-Geräten installierten Patches werden an den Administrationsserver übertragen. Das Aktivieren dieser Option kann die Auslastung des Administrationsservers und des DBMS erhöhen und eine Zunahme des Datenbankvolumens verursachen.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

Wenn das Ändern der in diesem Abschnitt angegebenen Einstellungen in der Richtlinie des Administrationsagenten unterbunden ist, können Sie diese Einstellungen nicht ändern.

Updates und Schwachstellen von Programmen

Im Abschnitt **Software-Updates und Schwachstellen** können Sie die Suche und Verteilung von Windows-Updates anpassen sowie die Untersuchung von ausführbaren Dateien auf Schwachstellen aktivieren:

- **Administrationsserver als WSUS-Server verwenden**

  Wenn diese Option aktiviert ist, werden die Windows-Updates auf den Administrationsserver heruntergeladen. Die heruntergeladenen Updates werden vom Administrationsserver zentralisiert für die Windows Update-Dienste mithilfe der Administrationsagenten auf den Client-Geräten bereitgestellt.

  Ist die Option deaktiviert, wird der Administrationsserver für den Download von Windows-Updates nicht verwendet. In diesem Fall erhalten die Client-Geräte die Windows-Updates selbständig.

  Diese Option ist standardmäßig deaktiviert.

- Unter **Benutzern die Verwaltung von Windows-Updates erlauben** können Sie Windows-Updates beschränken, die Benutzer auf ihren Geräten manuell mithilfe von Windows Update installieren können.

  Wenn auf Windows 10-Geräten der Windows Update-Dienst bereits Updates für das Gerät gefunden hat, wird die neue Option, die Sie unter **Benutzern die Verwaltung von Windows-Updates erlauben** auswählen können, erst angewendet, wenn die gefundenen Updates installiert wurden.

  Wählen Sie ein Element in der Dropdown-Liste:

  - **Benutzern die Installation aller anwendbaren Windows-Updates erlauben**

    Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar sind.

    Wählen Sie diese Option aus, wenn Sie nicht in die Installation von Updates eingreifen möchten.

    Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

  - **Benutzern nur die Installation von genehmigten Windows-Updates erlauben**

    Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar und die von Ihnen genehmigt sind.

    Beispielsweise können Sie zuerst die Installation von Updates in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb von Geräten nicht stören, und erst dann die Installation dieser genehmigten Updates auf Client-Geräten erlauben.

    Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

  - **Benutzern die Installation von Windows-Updates nicht erlauben**

    Benutzer können Microsoft Windows-Updates nicht manuell auf Ihren Geräten installieren. Alle anwendbaren Updates werden so installiert, wie sie von Ihnen angepasst wurden.

    Wählen Sie diese Variante aus, wenn Sie die Installation von Updates zentral verwalten möchten.

    Beispielsweise können Sie den Update-Zeitplan so optimieren, dass das Netzwerk nicht überlastet wird. Sie können Updates nach Büroschluss planen, damit sie sich nicht auf die Produktivität der Benutzer auswirken.

- In der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** können Sie den Modus für die Suche nach Updates auswählen:

  - **Aktiv**

    Wenn diese Option aktiviert ist, initiiert der Administrationsserver mit Unterstützung des Administrationsagenten eine Anfrage vom Windows Update-Agent des Client-Geräts zur Update-Quelle: Windows Update Server oder WSUS. Der Administrationsagent überträgt die vom Windows Update-Agent abgerufenen Daten an den Administrationsserver.

    Die Option wird nur wirksam, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** der Aufgabe *Finden von Schwachstellen und erforderlichen Updates* ausgewählt ist.

Diese Variante ist standardmäßig ausgewählt.

- **Offline**

  Bei Auswahl dieser Option überträgt der Administrationsagent regelmäßig Informationen über Updates, die bei der letzten Synchronisierung des Windows Update-Agent mit der Update-Quelle abgerufen wurden, vom Windows-Update-Agenten an den Administrationsserver. Wird die Synchronisierung des Windows Update-Agenten mit der Update-Quelle nicht ausgeführt, veralten die Daten über Updates auf dem Administrationsserver.

  Wählen Sie diese Option aus, wenn Sie Updates aus dem Speicher-Cache der Update-Quelle abrufen möchten.

- **Deaktiviert**

  Bei Auswahl dieser Option fragt der Administrationsserver keine Informationen über Updates ab.

  Wählen Sie diese Option aus, wenn Sie beispielsweise zuerst die Updates auf Ihrem lokalen Gerät testen möchten.

- **Ausführbare Dateien beim Start auf Schwachstellen untersuchen**

  Bei aktiviertem Kontrollkästchen werden ausführbare Dateien bei deren Start auf Schwachstellen untersucht.

  Diese Option ist standardmäßig aktiviert.

Verwaltung des Neustarts

Im Abschnitt **Verwaltung des Neustarts** können Sie die Aktion festlegen, die ausgeführt werden soll, wenn zur korrekten Ausführung, Installation oder Deinstallation des Programms ein Neustart des Betriebssystems des verwalteten Geräts erforderlich ist.

- **Betriebssystem nicht neu starten**

  Es wird kein Neustart des Betriebssystems durchgeführt.

- **Betriebssystem bei Bedarf automatisch neu starten**

  Bei Bedarf wird automatisch ein Neustart des Betriebssystems durchgeführt.

- **Benutzer fragen**

  Das Programm benötigt die Erlaubnis des Benutzers, um das Betriebssystem neu zu starten.

  Diese Variante ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen alle (Min.)**

    Wenn diese Option aktiviert ist, fordert das Programm den Benutzer in dem neben dem Kontrollkästchen angegebenen Intervall auf, das Betriebssystem neu zu starten. Standardeinstellungen beträgt das Intervall für eine erneute Aufforderung 5 Minuten.

    Ist die Option deaktiviert, fragt das Programm nicht erneut um Erlaubnis zum Neustart.

    Diese Option ist standardmäßig aktiviert.

  - **Neustart erzwingen nach (Min.)**

    Wenn diese Option aktiviert ist, wird nach der Aufforderung des Benutzers und Ablauf der im Feld neben dem Kontrollkästchen angegebenen Zeitspanne ein Neustart des Betriebssystems erzwungen.

    Ist die Option deaktiviert, erfolgt kein erzwungener Neustart.

Diese Option ist standardmäßig aktiviert.

- **Wartezeit vor dem erzwungenen Schließen von Programmen in gesperrten Sitzungen (Min.)**

  Programme werden zwangsweise geschlossen, wenn das Benutzergerät gesperrt wird (automatisch nach einer bestimmten Inaktivitätsdauer oder manuell).

  Wenn diese Option aktiviert ist, werden Programme auf einem gesperrten Gerät nach Ablauf der im Eingabefeld angegebenen Zeitspanne automatisch geschlossen.

  Wenn diese Option deaktiviert ist, werden Programme auf einem gesperrten Gerät nicht geschlossen.

  Diese Option ist standardmäßig deaktiviert.

Windows Desktopfreigabe

Im Abschnitt **Windows Desktopfreigabe** können Sie das Audit der Administrator-Tätigkeiten auf einem Remote-Gerät mit freigegebenem Desktop aktivieren und konfigurieren.

- **Audit aktivieren**

  Wenn diese Option aktiviert ist, dann ist das Audit des Administrators auf dem Remote-Gerät aktiviert. Einträge über die Aktionen des Administrators auf dem Remote-Gerät werden wie folgt gespeichert:

  - Im Ereignisprotokoll auf dem Remote-Gerät
  - In einer Datei mit der Erweiterung syslog, die sich im Installationsordner des Administrationsagenten auf dem Remote-Gerät befindet
  - In der Ereignisdatenbank von Kaspersky Security Center

  Das Audit des Administrators ist unter folgenden Bedingungen verfügbar:

  - Die Lizenz für das Schwachstellen- und Patch-Management wird verwendet
  - Der Administrator verfügt über die Berechtigung zum Start der Desktopfreigabe auf dem Remote-Gerät

  Wenn diese Option deaktiviert ist, dann ist das Audit des Administrators auf dem Remote-Gerät deaktiviert.

  Diese Option ist standardmäßig deaktiviert.

- **Masken der Dateien, die bei Lesezugriff überwacht werden sollen**

  Diese Liste enthält Dateimasken. Wenn das Audit aktiviert ist, verfolgt das Programm, welche Dateien der entsprechenden Masken vom Administrator gelesen werden, und speichert Informationen über das Lesen von Dateien. Die Liste ist verfügbar, wenn das Kontrollkästchen **Audit aktivieren** aktiviert ist. Die Dateimasken können geändert und neue Masken zur Liste hinzugefügt werden. Neue Dateimasken müssen in der Liste in einer neuen Zeile hinzugefügt werden.

  Standardmäßig sind die Dateimasken *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf angegeben.

- **Masken der Dateien, die auf Änderung überwacht werden sollen**

  Die Liste enthält die Dateimasken auf dem Remote-Gerät. Wenn das Audit aktiviert ist, verfolgt das Programm, welche Dateien der entsprechenden Masken vom Administrator geändert werden, und speichert Informationen über die Änderung der Dateien. Die Liste ist verfügbar, wenn das Kontrollkästchen **Audit aktivieren** aktiviert ist. Die Dateimasken können geändert und neue Masken zur Liste hinzugefügt werden. Neue Dateimasken müssen in der Liste in einer neuen Zeile hinzugefügt werden.

  Standardmäßig sind die Dateimasken *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf angegeben.

Verwaltung von Patches und Updates

Im Abschnitt **Verwaltung von Patches und Updates** können Sie das Abrufen und Verteilen der Updates sowie die Installation der Patches auf den verwalteten Geräten anpassen:

- **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**

  Ist diese Option aktiviert, so werden Kaspersky-Patches, die den Genehmigungsstatus *Nicht definiert* haben, sofort automatisch auf den verwalteten Geräten installiert, nachdem sie von den Update-Servern heruntergeladen wurden.

  Wenn die Option deaktiviert ist, werden die Patches von Kaspersky, die heruntergeladen und mit dem Status *Nicht festgestellt* markiert sind, erst installiert, wenn Sie ihren Status auf *Genehmigt* ändern.

  Diese Option ist standardmäßig aktiviert.

- **Updates und Antiviren-Datenbanken vom Administrationsserver vorab herunterladen (empfohlen)**

  Wenn diese Option aktiviert ist, wird das autonome Modell für das Abrufen von Updates verwendet. Wenn der Administrationsserver Updates empfängt, benachrichtigt der Administrationsagent (auf Geräten, auf denen er installiert ist) von den Updates, die für verwaltete Apps erforderlich sind. Wenn der Administrationsagent Informationen über diese Updates erhalten, ladet er die erforderlichen Dateien vom Administrationsserver im Voraus herunter. Bei der ersten Verbindung zum Administrationsagenten wird ein Updatedownload vom Administrationsserver initiiert. Nachdem der Administrationsagent alle Updates auf das Client-Gerät heruntergeladen hat, stehen die Updates den Programmen auf dem Gerät zur Verfügung.

  Wenn ein verwaltetes Programm auf dem Client-Gerät versucht, auf den Administrationsagenten zuzugreifen, um Updates herunterzuladen, überprüft der Administrationsagent, ob er über alle erforderlichen Updates verfügt. Wurden die Updates nicht mehr als 25 Stunden vor der Anfrage des verwalteten Programms vom Administrationsserver abgerufen, stellt der Administrationsagent keine Verbindung zum Administrationsserver her, sondern stellt dem verwalteten Programm die Updates aus dem lokalen Cache bereit. Eine Verbindung mit dem Administrationsserver wird möglicherweise nicht hergestellt, wenn der Administrationsagent Updates für Programme auf Client-Geräten bereitgestellt, für die Updates jedoch keine Verbindung erforderlich ist.

  Wenn diese Option deaktiviert ist, wird das autonome Modell für das Abrufen von Updates nicht verwendet. Updates werden gemäß dem Zeitplan der Aufgaben zum Update-Download verteilt.

  Diese Option ist standardmäßig aktiviert.

Konnektivität

Der Abschnitt **Konnektivität** beinhaltet drei untergeordnete Unterabschnitte:

- **Netzwerk**
- **Verbindungsprofile** (nur für Windows und macOS)
- **Verbindungszeitplan**

Im Unterabschnitt **Netzwerk** können Sie die Verbindungseinstellungen für den Administrationsserver konfigurieren, die Nutzung des UDP-Ports aktivieren und dessen Nummer festlegen. Es sind folgende Optionen verfügbar:

- In der Einstellungsgruppe **Verbindung mit dem Administrationsserver** können Sie die Verbindungseinstellungen für den Administrationsserver anpassen und das Synchronisierungsintervall der Client-Geräte mit dem Administrationsserver festlegen:

  - **Netzwerkverkehr komprimieren**

    Aktivieren Sie diese Option, um die Geschwindigkeit der Datenübertragung durch den Administrationsagenten zu steigern, das Datenvolumen zu komprimieren und die Belastung für den Administrationsserver zu reduzieren.

    > Die CPU-Auslastung des Client-Computers kann ansteigen.

    Dieses Kontrollkästchen ist standardmäßig aktiviert.

  - **Ports des Administrationsagenten in der Windows-Firewall öffnen**

    Wenn diese Option aktiviert ist, werden die Ports, die für die Arbeit des Administrationsagenten erforderlich sind, zur Ausschlussliste der Microsoft Windows Firewall hinzugefügt.

    Diese Option ist standardmäßig aktiviert.

  - **SSL verwenden**

    Wenn diese Option aktiviert ist, erfolgt die Verbindung zum Administrationsserver über einen gesicherten Port mit SSL-Protokoll.

    Diese Option ist standardmäßig aktiviert.

  - **Verbindungs-Gateway auf Verteilungspunkt (falls vorhanden) unter Standard-Verbindungseinstellungen verwenden**

    Wenn die Option aktiviert ist, wird das Verbindungs-Gateway auf dem Verteilungspunkt mit den Einstellungen verwendet, die in den Administrationsgruppeneigenschaften festgelegt sind.

    Diese Option ist standardmäßig aktiviert.

- **UDP-Port verwenden**

  Wenn es erforderlich ist, dass sich der Administrationsagent über einen UDP-Port mit dem Administrationsserver verbindet, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine **UDP-Portnummer** an. Diese Option ist standardmäßig aktiviert. Der standardmäßige UDP-Port für die Verbindung zum Administrationsserver ist 15000.

- **UDP-Port**

  Im Eingabefeld können Sie die Nummer des UDP-Ports eingeben. Standardmäßig wird Portnummer 15000 verwendet.

  Für die Eingabe wird das Dezimalformat verwendet.

  Wenn auf einem Client-Gerät das Betriebssystem Microsoft Windows XP Service Pack 2 installiert ist, blockiert die integrierte Firewall den UDP-Port mit der Nummer 15000. In diesem Fall muss der Port manuell geöffnet werden.

- **Verbindung zum Administrationsserver mittels Verteilungspunkt erzwingen**

  Wählen Sie diese Option, wenn Sie im Fenster mit den Einstellungen des Verteilungspunktes die Option **Diesen Verteilungspunkt als Push-Server verwenden** ausgewählt haben. Andernfalls wird der Verteilungspunkt nicht als Push-Server fungieren.

Im Unterabschnitt **Verbindungsprofile** können Sie die Einstellungen des Netzwerkspeicherorts angeben, die Profile für die Verbindung mit dem Administrationsserver konfigurieren und den Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist.

- **Einstellungen des Netzwerkstandorts**

  Die Einstellungen des Netzwerkspeicherorts bestimmen die Merkmale des Netzwerks, mit dem das Client-Gerät verbunden ist, und legen die Regeln für den Wechsel des Administrationsagenten von einem Administrationsserver-Verbindungsprofil zu einem anderen fest (im Falle sich ändernder Merkmale des Netzwerks).

- **Verbindungsprofile des Administrationsservers**

  In diesem Abschnitt können Sie ein Profil für die Verbindung des Administrationsagenten mit dem Administrationsserver anzeigen und hinzufügen. In diesem Abschnitt können ferner die Umschaltregeln des Administrationsagenten auf andere Administrationsserver im Fall des Auftretens folgender Ereignisse festgelegt werden:

  - Verbindung des Client-Geräts mit einem anderen lokalen Netzwerk.
  - Trennung der Verbindung des Geräts vom lokalen Unternehmensnetzwerk.
  - Änderung der Verbindungs-Gateway-Adresse oder der Adresse des DNS-Servers.

  > Verbindungsprofile werden nur für Geräte mir Windows oder macOS unterstützt.

- **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**

  Wenn diese Option aktiviert ist, und eine Verbindung über dieses Profil besteht, verwenden Programme, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte im Modus für mobile Benutzer sowie Richtlinien für mobile Benutzer. Wurde für die Anwendung keine Richtlinie für mobile Benutzer definiert, verwendet die Anwendung die aktive Richtlinie.

  Wenn diese Option deaktiviert ist, wenden die Anwendungen die aktiven Richtlinien an.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Verbindungszeitplan** können Sie Zeitintervalle festlegen, in denen der Administrationsagent Daten auf den Administrationsserver übertragen soll:

- **Verbindung bei Bedarf herstellen**

  Bei dieser Variante wird eine Verbindung dann hergestellt, wenn Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen.

  Diese Variante ist standardmäßig ausgewählt.

- **Verbindung in den angegebenen Zeiträumen herstellen**

  Bei dieser Variante wird eine Verbindung des Administrationsagenten mit dem Administrationsserver in den vorgegebenen Zeiträumen hergestellt. Sie können mehrere Zeiträume für die Verbindung hinzufügen.

Verteilungspunkte

Der Abschnitt **Verteilungspunkte** beinhaltet vier untergeordnete Unterabschnitte:

- **Netzwerk durchsuchen**
- **Einstellungen der Internetverbindung**
- **KSN Proxy**
- **Updates**

Im Unterabschnitt **Netzwerk durchsuchen** können Sie die automatische Abfrage des Netzwerks anpassen. Sie können drei Arten von Abfragen aktivieren: Netzwerkabfragen, Abfragen eines IP-Bereichs und Abfragen des Active Directory:

- **Netzwerkabfrage erlauben**

  Wenn diese Option aktiviert ist, fragt der Administrationsserver das Netzwerk automatisch gemäß dem Zeitplan ab, den Sie über die Links **Zeitplan für schnelle Abfrage festlegen** und **Zeitplan für vollständige Abfrage festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver das Netzwerk mit jenem Intervall ab, das im Feld **Intervall für Netzwerkabfragen (Min.)** angegeben ist.

  Das Intervall der Gerätesuche kann für Versionen des Administrationsagenten bis Version 10.2 in den Feldern **Intervall für Abfrage von Windows-Domänen (Min.)** (für schnelle Abfragen eines Windows-Netzwerks) und **Intervall für Netzwerkabfragen (Min.)** (für vollständige Abfragen eines Windows-Netzwerks) angepasst werden.

  Diese Option ist standardmäßig deaktiviert.

- **Abfrage des IP-Bereichs zulassen**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt die IP-Bereiche automatisch gemäß dem Zeitplan ab, den Sie über die Schaltfläche **Abfragezeitplan festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt keine IP-Bereiche ab.

  Das Intervall der Abfrage des IP-Bereichs kann für Versionen des Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Abschnitt ist verfügbar, wenn die Option aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

- **Zeroconf-Abfragen verwenden (nur auf Linux-Plattformen; manuell angegebene IP-Bereiche werden ignoriert)**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt das Netzwerk mit IPv6-Geräten unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) automatisch ab. In diesem Fall werden aktivierte IP-Bereichsabfragen ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt.

  Um Zeroconf verwenden zu können, müssen die folgenden Bedingungen erfüllt sein:

  - Der Verteilungspunkt muss unter Linux laufen.
  - Sie müssen auf dem Verteilungspunkt das Tool "avahi-browse" installieren.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt Netzwerke mit IPv6-Geräten nicht ab.

  Diese Option ist standardmäßig deaktiviert.

- **Abfrage des Active Directory zulassen**

  Wenn diese Option aktiviert ist, führt der Verteilungspunkt automatisch eine Abfrage des Active Directory gemäß dem Zeitplan durch, den Sie über den Link **Abfragezeitplan festlegen** eingestellt haben.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver das Active Directory nicht ab.

  Das Intervall der Abfrage des Active Directory kann für Versionen des Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Feld ist verfügbar, wenn diese Option aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

Wenn Ihre Verteilungspunkte für die Verbindung mit dem Internet einen Proxyserver verwenden, können Sie im Unterabschnitt **Einstellungen für die Internetverbindung** die folgenden Einstellungen festlegen:

- **Proxyserver verwenden**

  Wenn Sie das Kontrollkästchen aktivieren, können Sie in den Eingabefeldern die Verbindungseinstellungen zum Proxyserver angeben.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Proxyserver-Adresse**

  Proxyserver-Adresse.

- **Port**

  Nummer des Ports, über den die Verbindung erfolgt.

- **Proxyserver für lokale Adressen umgehen**

  Wenn die Option aktiviert ist, wird bei der Verbindung mit den Geräten im lokalen Netzwerk kein Proxyserver verwendet.

  Diese Option ist standardmäßig deaktiviert.

- **Authentifizierung am Proxyserver**

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Benutzername**

  Benutzerkonto, unter dessen Namen die Verbindung mit dem Proxy-Server hergestellt wird.

- **Kennwort**

  Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

Im Unterabschnitt **KSN Proxy** können Sie das Programm anpassen, um den Verteilungspunkt zum Weiterleiten von KSN-Anfragen von den verwalteten Geräten zu verwenden:

- **KSN Proxy auf dem Verteilungspunkt aktivieren**

  Der KSN-Proxy-Service wird auf dem Gerät ausgeführt, das als Verteilungspunkt verwendet wird. Verwenden Sie diese Funktion, um Datenverkehr im Netzwerk neu zu verteilen und zu optimieren.

  Der Verteilungspunkt sendet die KSN-Statistik, die in der Erklärung zu Kaspersky Security Network aufgeführt sind, an Kaspersky.

Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn im Fenster mit den Eigenschaften des Administrationsservers die Optionen **Administrationsserver als Proxyserver verwenden** und **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** aktiviert sind.

Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

- **KSN-Anfragen an den Administrationsserver weiterleiten**

  Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an den Administrationsserver weiter.

  Diese Option ist standardmäßig aktiviert.

- **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**

  Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an die KSN Cloud oder an KPSN weiter. KSN-Anfragen, die der Verteilungspunkt selbst generiert, werden ebenso direkt an KSN Cloud oder KPSN gesendet.

  Verteilungspunkte, auf denen der Administrationsagent bis einschließlich Version 11 installiert ist, können nicht direkt auf KPSN zugreifen. Um die Verteilungspunkte so anzupassen, dass KSN-Anfragen an KPSN gesendet werden, aktivieren Sie für jeden Verteilungspunkt die Option **KSN-Anfragen an den Administrationsserver weiterleiten**.

  Verteilungspunkte, auf denen der Administrationsagent ab Version 12 installiert ist, können direkt auf KPSN zugreifen.

- **TCP-Port**

  Die Nummer des TCP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Standardmäßig wird Portnummer 13111 verwendet.

- **UDP-Port verwenden**

  Wenn es erforderlich ist, dass sich der Administrationsagent über einen UDP-Port mit dem Administrationsserver verbindet, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine **UDP-Portnummer** an. Diese Option ist standardmäßig aktiviert. Der standardmäßige UDP-Port für die Verbindung zum Administrationsserver ist 15000.

In dem Unterabschnitt **Updates** können Sie durch Aktivieren oder Deaktivieren der Option **Diff-Dateien herunterladen** angeben, ob der Administrationsagent Diff-Dateien herunterladen soll (Diese Option ist standardmäßig aktiviert).

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie den Revisionsverlauf für die Richtlinien des Administrationsagenten anzeigen. Sie können Revisionen vergleichen, Revisionen ansehen und erweiterte Aktionen ausführen, z. B. Revisionen in einer Datei speichern, ein Rollback auf eine bestimmte Revision vornehmen und Beschreibungen von Revisionen hinzufügen und ändern.

Benutzerkonten verwalten

Dieser Abschnitt enthält Informationen über die Benutzerkonten und Benutzerrollen, die vom Programm unterstützt werden. Es umfasst Anleitungen zur Erstellung von Benutzerkonten und Benutzerrollen für Kaspersky Security Center.

In Kaspersky Security Center können Benutzerkonten und Gruppen von Benutzerkonten verwaltet werden. Das Programm unterstützt drei Arten von Benutzerkonten:

- Benutzerkonten für Mitarbeiter einer Organisation. Der Administrationsserver erhält Daten über die Konten dieser Domänenbenutzer beim Abfragen des Domänencontrollers des Unternehmens.
- Benutzerkonten für lokale Benutzer. Lokale Benutzerkonten auf verwalteten Geräten sowie lokale Benutzerkonten auf dem Gerät mit dem installiertem Administrationsserver.
- Benutzerkonten für interne Benutzer von Kaspersky Security Center. Sie können Konten von internen Benutzern erstellen. Diese Benutzerkonten werden nur innerhalb von Kaspersky Security Center verwendet.

Arbeiten mit Benutzerkonten

In Kaspersky Security Center können Benutzerkonten und Gruppen von Benutzerkonten verwaltet werden. Das Programm unterstützt zwei Typen von Benutzerkonten:

- Benutzerkonten der Mitarbeiter einer Organisation. Der Administrationsserver erhält Daten über die Benutzerkonten dieser Benutzer beim Abfragen des Unternehmensnetzwerks.
- Benutzerkonten für interne Benutzer. Diese werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Benutzerkonten für interne Benutzer werden nur innerhalb von Kaspersky Security Center erstellt und verwendet.

Sie können die Liste der Benutzerkonten auf eine der folgenden Arten anzeigen:

- Wechseln Sie in der Konsolenstruktur zu **Erweitert** → **Benutzerkonten**.
- Wechseln Sie in der Konsolenstruktur zum Abschnitt **Verwaltete Geräte** → Registerkarte **Geräte** → Link <Gerätename> → **Sitzungen**.

  Im Abschnitt **Sitzungen** werden Benutzerkonten mit aktiven Sitzungen auf Windows-Geräten angezeigt.

Die Liste der Benutzerkonten wird korrekt angezeigt, wenn die folgenden Voraussetzungen erfüllt sind:

- Sie verwenden den Administrationsagenten in der gleichen Version (oder höher) wie den Administrationsserver.
- Die Active Directory-Abfrage ist aktiviert, um die Benutzerkonten der Domänenbenutzer anzuzeigen.
- Auf verwalteten Windows-Geräten wird der Dienst **Server (LanmanServer)** ausgeführt.

Mit Benutzerkonten und Benutzergruppen können folgenden Aktionen ausgeführt werden:

- Zugriffsrechte der Benutzer für die Programmfunktionen mithilfe von Rollen anpassen.
- Nachrichten mithilfe von E-Mail oder SMS an Benutzer senden.
- Liste der mobilen Geräte des Benutzers anzeigen.
- Zertifikate ausstellen und auf den mobilen Geräten der Benutzer installieren.
- Liste der für den Benutzer ausgestellten Zertifikate anzeigen.
- Die zweistufige Überprüfung für ein Benutzerkonto deaktivieren.

Hinzufügen eines Benutzerkontos eines internen Benutzers

So fügen Sie ein neues internes Benutzerkonto zum Kaspersky Security Center hinzu:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Benutzerkonten**.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Klicken Sie im Arbeitsbereich auf die Schaltfläche **Benutzer hinzufügen**.

3. Geben Sie im folgenden Fenster **Neuer Benutzer** die Einstellungen des neuen Benutzerkontos an:

   - Einen Benutzernamen ()

     Gehen Sie bei der Eingabe des Benutzernamens umsichtig vor. Sie können es nach dem Speichern der Änderungen nicht mehr ändern.

   - **Beschreibung**
   - **Vollständiger Name**
   - **Haupt-E-Mail-Adresse**
   - **Hauptrufnummer**
   - **Kennwort** für die Verbindung des Benutzers mit Kaspersky Security Center

     Das Kennwort muss den folgenden Regeln entsprechen:

     - Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
     - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
       - Großbuchstaben (A–Z)
       - Kleinbuchstaben (a–z)
       - Ziffern (0–9)
       - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

     Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen**.

     Die Anzahl der Eingabeversuche für das Kennwort ist beschränkt. Standardmäßig beträgt die maximale Anzahl der Eingabeversuche für das Kennwort 10. Sie können die zulässige Anzahl der Versuche zur Eingabe eines Kennworts ändern (siehe Beschreibung unter Anzahl der erlaubten Kennworteingabeversuche).

Wenn der Benutzer das Kennwort innerhalb der angegebenen Anzahl von Versuchen nicht korrekt eingegeben hat, wird das Benutzerkonto für eine Stunde gesperrt. In der Liste der Benutzerkonten ist das Icon () des Benutzers eines blockierten Benutzerkontos abgeblendet (nicht verfügbar). Sie können das Benutzerkonto nur durch die Änderung des Kennworts entsperren.

- Aktivieren Sie ggf. das Kontrollkästchen **Benutzerkonto deaktivieren**, um zu verhindern, dass der Benutzer eine Verbindung zur Anwendung herstellt. Sie können beispielsweise ein Konto deaktivieren, wenn Sie es zuvor erstellen, aber später aktivieren möchten.

- Markieren Sie das Kontrollkästchen **Ändern der Kontoeinstellungen nur mit Kennwort möglich**, um eine zusätzliche Option zu aktivieren, die ein Benutzerkonto vor unbefugten Änderungen schützt. Wenn diese Option aktiviert ist, erfordert das Ändern der Benutzerkontoeinstellungen die Autorisierung des Benutzers mit Berechtigungen zum Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**.

4. Klicken Sie auf die Schaltfläche **OK**.

Das neu erstellte Benutzerkonto wird im Arbeitsbereich des Ordners **Benutzerkonten** angezeigt.

Bearbeiten eines Benutzerkontos eines internen Benutzers

So bearbeiten Sie ein internes Benutzerkonto in Kaspersky Security Center:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Benutzerkonten**.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Doppelklicken Sie im Arbeitsbereich auf das interne Benutzerkonto, das Sie bearbeiten möchten.

3. Ändern Sie im folgenden Fenster **Eigenschaften: <Benutzername>** die Einstellungen des Benutzerkontos:

   - **Beschreibung**
   - **Vollständiger Name**
   - **Haupt-E-Mail-Adresse**
   - **Hauptrufnummer**
   - **Kennwort** für die Verbindung des Benutzers mit Kaspersky Security Center

     Das Kennwort muss den folgenden Regeln entsprechen:

     - Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
     - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
       - Großbuchstaben (A–Z)
       - Kleinbuchstaben (a–z)

- Ziffern (0–9)
- Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen**.

Die Anzahl der Eingabeversuche für das Kennwort ist beschränkt. Standardmäßig beträgt die maximale Anzahl der Eingabeversuche für das Kennwort 10. Sie können die zulässige Anzahl der Versuche zur Eingabe eines Kennworts ändern (siehe Beschreibung unter Anzahl der erlaubten Kennworteingabeversuche).

Wenn der Benutzer das Kennwort innerhalb der angegebenen Anzahl von Versuchen nicht korrekt eingegeben hat, wird das Benutzerkonto für eine Stunde gesperrt. In der Liste der Benutzerkonten ist das Icon () des Benutzers eines blockierten Benutzerkontos abgeblendet (nicht verfügbar). Sie können das Benutzerkonto nur durch die Änderung des Kennworts entsperren.

- Aktivieren Sie ggf. das Kontrollkästchen **Benutzerkonto deaktivieren**, um zu verhindern, dass der Benutzer eine Verbindung zur Anwendung herstellt. Sie können ein Konto beispielsweise deaktivieren, nachdem ein Mitarbeiter das Unternehmen verlassen hat.
- Wählen Sie die Option **Ändern der Kontoeinstellungen nur mit Kennwort möglich**, um eine zusätzliche Option zu aktivieren, die ein Benutzerkonto vor unbefugten Änderungen schützt. Wenn diese Option aktiviert ist, erfordert das Ändern der Benutzerkontoeinstellungen die Autorisierung des Benutzers mit Berechtigungen zum Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**.

4. Klicken Sie auf die Schaltfläche **OK**.

Das bearbeitete Benutzerkonto wird im Arbeitsbereich des Ordners **Benutzerkonten** angezeigt.

Ändern der Anzahl der zulässigen Kennworteingabeversuche

Benutzer von Kaspersky Security Center können eine begrenzte Anzahl von ungültigen Kennwörtern eingeben. Wenn das Limit erreicht ist, wird das Benutzerkonto für eine Stunde gesperrt.

Standardmäßig liegt die maximale Anzahl zulässiger Versuche zur Eingabe eines Kennworts bei 10. Sie können die Anzahl der zulässigen Kennworteingabeversuche ändern (siehe Beschreibung in diesem Abschnitt).

So ändern Sie die Anzahl der zulässigen Kennworteingabeversuche:

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsserver installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** > **Ausführen**.
2. Rufen Sie den folgenden Schlüssel auf:
   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

- Für 64-Bit-Systeme:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Wenn der SrvSplPpcLogonAttempts-Wert nicht vorhanden ist, erstellen Sie ihn. Der Typ des Werts lautet DWORD.

   Nach der Installation von Kaspersky Security Center wird dieser Wert standardmäßig nicht erstellt.

4. Geben Sie die erforderliche Anzahl von Versuchen im SrvSplPpcLogonAttempts-Wert an.

5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

6. Starten Sie den Dienst des Administrationsservers neu.

Die maximale Anzahl der Eingabeversuche für das Kennwort wird geändert.

Prüfung der Eindeutigkeit des Namens des internen Benutzers anpassen

Sie können die Prüfung der Eindeutigkeit des Namens des internen Benutzers von Kaspersky Security Center bei seinem Hinzufügen zum Programm anpassen. Die Prüfung der Eindeutigkeit des Namens des internen Benutzers kann nur auf dem virtuellen Administrationsserver oder dem primären Administrationsserver ausgeführt werden, für den das Benutzerkonto erstellt wird, bzw. auf allen virtuellen Servern und dem primären Administrationsserver. Standardmäßig wird die Prüfung der Eindeutigkeit des Namens des internen Benutzers auf allen virtuellen Administrationsservern und auf dem primären Administrationsserver ausgeführt.

Um die Prüfung der Eindeutigkeit des Namens des internen Benutzers im Rahmen des virtuellen Administrationsservers oder des primären Administrationsservers zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsserver installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** > **Ausführen**.

2. Rufen Sie den folgenden Abschnitt auf:

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM.

   - Für 64-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Für den Schlüssel LP_InterUserUniqVsScope (DWORD) ist der Wert 00000001 festgelegt.

   Standardmäßig wird für diesen Schlüssel der Wert 0 festgelegt.

4. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin wird die Prüfung der Namenseindeutigkeit nur auf jenem virtuellen Administrationsserver ausgeführt, auf dem der interne Benutzer erstellt wurde, bzw. auf dem primären Administrationsserver, wenn der Benutzer auf dem primären Administrationsserver erstellt wurde.

Um die Prüfung der Eindeutigkeit des Namens des internen Benutzers auf allen virtuellen Administrationsservern und dem primären Administrationsserver zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsserver installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** > **Ausführen**.
2. Rufen Sie den folgenden Abschnitt auf:
   - Für 64-Bit-Systeme:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - Für 32-Bit-Systeme:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM.
3. Für den Schlüssel LP_InterUserUniqVsScope (DWORD) ist der Wert 00000000 festgelegt.
   Standardmäßig wird für diesen Schlüssel der Wert 0 festgelegt.
4. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin wird die Prüfung der Eindeutigkeit des Namens des internen Benutzers auf allen virtuellen Administrationsservern und auf dem primären Administrationsserver ausgeführt.

Sicherheitsgruppen hinzufügen

Sie können Sicherheitsgruppen (Benutzergruppen) hinzufügen und den Umfang der Gruppen sowie den Zugriff einer Sicherheitsgruppe zu den verschiedenen Programmfunktionen flexibel konfigurieren. Die Sicherheitsgruppen können einen ihrem Verwendungszweck entsprechenden Namen erhalten. Der Name kann beispielsweise dem Standort der Benutzer im Büro oder der Bezeichnung einer Unternehmensabteilung entsprechen, zu der die Benutzer gehören.

Ein Benutzer kann Teil mehrerer Sicherheitsgruppen sein. Das Benutzerkonto eines Benutzers unter der Verwaltung eines virtuellen Administrationsservers kann nur zu Sicherheitsgruppen dieses virtuellen Servers gehören und verfügt nur über die im Rahmen dieses virtuellen Servers vorgesehenen Zugriffsrechte.

Um eine Sicherheitsgruppen hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** aus.
   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.
2. Klicken Sie auf die Schaltfläche **Sicherheitsgruppe hinzufügen**.
   Das Fenster **Sicherheitsgruppe hinzufügen** wird geöffnet.
3. Geben Sie im Fenster **Sicherheitsgruppe hinzufügen** im Abschnitt **Allgemein** den Gruppennamen an.
   Der Gruppenname darf nicht mehr als 255 Zeichen umfassen und die Zeichen *, <, >, ?, \, :, | nicht enthalten. Der Gruppenname muss eindeutig sein.
   Sie können im Eingabefeld **Beschreibung** eine Beschreibung der Gruppe eingeben. Das Feld **Beschreibung** muss nicht verpflichtend ausgefüllt werden.
4. Klicken Sie auf die Schaltfläche **OK**.

Die hinzugefügte Sicherheitsgruppen wird in der Konsolenstruktur im Ordner **Benutzerkonten** angezeigt. Sie können Benutzer zur erstellte Gruppe hinzufügen.

Benutzer zur Gruppe hinzufügen

Gehen Sie folgendermaßen vor, um einen Benutzer zur Gruppe hinzuzufügen:

1. Wählen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** aus.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Wählen Sie in der Liste der Benutzerkonten und Gruppen die Gruppe, zu der ein Benutzer hinzugefügt werden soll.

3. Wählen Sie im Eigenschaftenfenster der Gruppe den Abschnitt **Gruppenbenutzer** aus und klicken Sie dann auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird ein Fenster mit einer Benutzerliste geöffnet.

4. Wählen Sie den Benutzer, den Sie in die Gruppe aufnehmen möchten, aus der Liste aus.

5. Klicken Sie auf die Schaltfläche **OK**.

Der Benutzer wird zur Gruppe hinzugefügt und in der Liste der Gruppenbenutzer angezeigt.

Zugriffsrechte auf Programmfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle

Kaspersky Security Center bietet Unterstützungen für eine rollenbasierte Zugriffskontrolle auf die Funktionen von Kaspersky Security Center und von verwalteten Kaspersky-Anwendungen an.

Sie können die Zugriffsrechte auf Programmfunktionen für Benutzer von Kaspersky Security Center mit einer der folgenden Methoden konfigurieren:

- Durch individuelle Konfiguration der Berechtigungen jedes Benutzers bzw. jeder Benutzergruppe.
- Durch Erstellen typischer Benutzerrollen mit einer vordefinierten Auswahl von Berechtigungen und Zuweisung der Rollen an die Benutzer entsprechend ihrer dienstlichen Verpflichtungen.

Eine *Benutzerrolle* (aus als "Rolle" bezeichnet) ist eine vordefinierte Menge an Berechtigungen für Funktionen von Kaspersky Security Center oder von verwalteten Kaspersky-Anwendungen. Die Rolle kann einem Benutzer oder einer Benutzergruppe zugewiesen werden.

Die Verwendung von Benutzerrollen soll die stets wiederkehrenden Abläufe für das Konfigurieren von Zugriffsrechten der Benutzer auf Programmfunktionen vereinfachen und verkürzen. Die Zugriffsberechtigungen werden in einer Rolle nach den typischen Aufgaben und Verantwortungsbereichen des Benutzers festgelegt.

Die Benutzerrollen können nach dem jeweiligen Verwendungszweck benannt werden. Sie können eine unbegrenzte Anzahl von Rollen in der Anwendung erstellen.

Sie können entweder vordefinierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen und die notwendigen Berechtigungen selbst konfigurieren.

Zugriffsrechte auf Programmfunktionen

Die untenstehende Tabelle gibt die Funktionen von Kaspersky Security Center mit den Zugriffsrechten für die Verwaltung der damit verknüpften Aufgaben, Berichte und Einstellungen, sowie für das Durchführen der damit verknüpften Benutzervorgänge an.

Um einen in der Tabelle aufgeführten Vorgang auszuführen, muss ein Benutzer die rechts neben dem Vorgang angegebene Berechtigung besitzen.

Die Berechtigungen **Lesen**, **Schreiben** und **Ausführen** können auf jede Aufgabe, jeden Bericht und jede Einstellung angewendet werden. Zusätzlich zu diesen Berechtigungen muss ein Benutzer über die Berechtigung **Vorgänge für die Geräteauswahlen ausführen** verfügen, um Aufgaben, Berichte oder Einstellungen auf Geräteauswahlen zu verwalten.

Alle Aufgaben, Berichte, Einstellungen und Installationspakete, die in der Tabelle fehlen, gehören zum Funktionsbereich **Allgemeine Funktionen: Basisfunktionen**.

Zugriffsrechte auf Programmfunktionen

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: Verwaltung von Administrationsgruppen	**Schreiben**	• Hinzufügen eines Geräts zu einer Administrationsgruppe: **Schreiben** • Löschen eines Geräts aus einer Administrationsgruppe: **Schreiben** • Hinzufügen einer Administrationsgruppe zu einer anderen Administrationsgruppe: **Schreiben** • Löschen einer Administrationsgruppe aus einer anderen Administrationsgruppe: **Schreiben**	Keine

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: Auf Objekte unabhängig von ihren ACLs zugreifen	**Lesen**	Lesen auf alle Objekte erhalten: **Lesen**	Keine
Allgemeine Funktionen: Basisfunktionen	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Regeln für das Verschieben von Geräten (erstellen, ändern, löschen) für den virtuellen Server: **Schreiben**, **Vorgänge für die Geräteauswahlen ausführen** • Benutzerdefiniertes Zertifikat des Mobilfunkprotokolls (LWNGT) erhalten: **Lesen** • Benutzerdefiniertes Zertifikat des Mobilfunkprotokolls (LWNGT) festlegen: **Schreiben** • NLA-definierte Netzwerkliste erhalten: **Lesen** • NLA-definierte Netzwerkliste hinzufügen, ändern oder löschen: **Schreiben** • Liste der Zugriffskontrolle von Gruppen anzeigen: **Lesen** • Kaspersky-Ereignisprotokoll anzeigen: **Lesen** • Anzeigen des Wiederherstellungsschlüssels, um den Zugriff auf eine mit BitLocker-Laufwerkverschlüsselung verschlüsselte Festplatte wiederherzustellen: **Ausführen**	• "Download von in die Datenver des Administrations • "Berichte sende • "Installationspa verteilen" • "Remote-Install einer Anwendu sekundären Administrations
Allgemeine Funktionen: Gelöschte Objekte	• **Lesen** • **Schreiben**	• Gelöschte Objekte im Papierkorb anzeigen: **Lesen** • Objekte aus dem Papierkorb löschen: **Schreiben**	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: Verarbeitung von Ereignissen	• **Ereignisse löschen** • **Ereignisbenachrichtigungseinstellungen bearbeiten** • **Ereignisprotokollierungseinstellungen bearbeiten** • **Schreiben**	• Einstellungen der Ereignisregistrierung ändern: **Ereignisprotokollierungseinstellungen bearbeiten** • Einstellungen der Ereignisbenachrichtigung ändern: **Ereignisbenachrichtigungseinstellungen bearbeiten** • Ereignisse löschen: **Ereignisse löschen**	Nichts
Allgemeine Funktionen: Vorgänge mit dem Administrationsserver	• **Lesen** • **Schreiben** • **Ausführen** • **Objekt-ACLs ändern** • **Vorgänge für die Geräteauswahlen ausführen**	• Ports des Administrationsservers für die Verbindung zum Administrationsagenten angeben: **Schreiben** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy angeben: **Schreiben** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy für mobile Geräte angeben: **Schreiben** • Ports des Webservers für die Verteilung von autonomen Paketen angeben: **Schreiben** • Ports des Webservers für die Verteilung von MDM-Profilen angeben: **Schreiben** • SSL-Ports des Administrationsservers für die Verbindung mittels Kaspersky Security Center Web Console angeben: **Schreiben** • Ports des Administrationsservers für die Verbindung mit mobilen Geräten angeben: **Schreiben** • Maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind, angeben: **Schreiben** • Maximale Anzahl von Ereignissen, die der Administrationsserver versenden kann, angeben: **Schreiben** • Zeitspanne, in welcher Ereignisse durch den Administrationsserver versendet werden können, angeben: **Schreiben**	• "Backup der Da Administrations anlegen" • "Pflege von Datenbanken"
Allgemeine Funktionen: Bereitstellen von Kaspersky-Anwendungen	• **Patches von Kaspersky verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	Die Installation von Patches akzeptieren oder ablehnen: **Patches von Kaspersky verwalten**	Nichts
Allgemeine Funktionen: Lizenzschlüsselverwaltung	• **Schlüsseldatei exportieren** • **Schreiben**	• Schlüsseldatei exportieren: **Schlüsseldatei exportieren** • Einstellungen des Lizenzschlüssels des Administrationsservers ändern:	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
		Schreiben	
Allgemeine Funktionen: Erzwungene Berichtsverwaltung	• **Lesen** • **Schreiben**	• Berichte unabhängig von ihren ACLs erstellen: **Schreiben** • Berichte unabhängig von ihren ACLs exportieren: **Lesen**	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: Hierarchie der Administrationsserver	**Hierarchie der Administrationsserver konfigurieren**	Sekundäre Administrationsserver registrieren, aktualisieren oder löschen: **Hierarchie der Administrationsserver konfigurieren**	Nichts
Allgemeine Funktionen: Benutzerberechtigungen	**Objekt-ACLs ändern**	• "Sicherheit"-Eigenschaften eines jeden Objekts ändern: **Objekt-ACLs ändern** • Benutzerrollen verwalten: **Objekt-ACLs ändern** • Interne Benutzer verwalten: **Objekt-ACLs ändern** • Sicherheitsgruppen verwalten: **Objekt-ACLs ändern** • Anmeldenamen verwalten: **Objekt-ACLs ändern**	Nichts
Allgemeine Funktionen: Virtuelle Administrationsserver	• **Virtuelle Administrationsserver verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Liste mit virtuellen Administrationsservern abrufen: **Lesen** • Informationen über den virtuellen Administrationsserver erhalten: **Lesen** • Virtuellen Administrationsserver erstellen, aktualisieren oder löschen: **Virtuelle Administrationsserver verwalten** • Virtuellen Administrationsserver in andere Gruppe verschieben: **Virtuelle Administrationsserver verwalten** • Rechte des virtuellen Administrationsservers angeben: **Virtuelle Administrationsserver verwalten**	Nichts
Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel	• **Lesen** • **Schreiben**	• Exportieren von Chiffrierschlüsseln: **Lesen** • Importieren von Chiffrierschlüsseln: **Schreiben**	Nichts
Verwaltung mobiler Geräte: Allgemein	• **Neue Geräte verbinden** • **Nur informative Befehle an mobile Geräte senden** • **Befehle an mobile Geräte senden** • **Zertifikate verwalten** • **Lesen** • **Schreiben**	• Wiederherstellungsdaten des Schlüsselverwaltungsdienstes abrufen: **Lesen** • Benutzerzertifikate löschen: **Zertifikate verwalten** • Öffentlichen Teil eines Benutzerzertifikats abrufen: **Lesen** • Aktivierung der Public-Key-Infrastruktur prüfen: **Lesen** • Konto der Public-Key-Infrastruktur prüfen: **Lesen** • Vorlagen der Public-Key-Infrastruktur abrufen: **Lesen** • Vorlagen der Public-Key-Infrastruktur nach Zertifikat der "Extended Key Usage" abrufen: **Lesen** • Widerruf des Zertifikats der Public-Key-Infrastruktur prüfen: **Lesen** • Einstellungen für die Ausstellung von Benutzerzertifikaten aktualisieren: **Zertifikate verwalten** • Einstellungen für die Ausstellung von Benutzerzertifikaten abrufen: **Lesen** • Pakete nach Programmname und Version abrufen: **Lesen** • Benutzerzertifikate einstellen oder abbrechen: **Zertifikate verwalten** • Benutzerzertifikate erneuern: **Zertifikate verwalten** • Tags für Benutzerzertifikate einstellen: **Zertifikate verwalten** • Erzeugung von MDM-Installationspaketen ausführen / abbrechen: **Neue Geräte verbinden**	Nichts
Systemverwaltung: Konnektivität	• **RDP-Sitzungen starten** • **Mit vorhandenen RDP-Sitzungen verbinden** • **Tunnelung starten**	• Sitzung für Desktopfreigabe erstellen: **RDP-Sitzungen starten** • RDP-Sitzungen erstellen: **Mit vorhandenen RDP-Sitzungen verbinden**	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
	• **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Tunnel erstellen: **Tunnelung starten** • Liste mit Content-Netzwerken speichern: **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern**	
Systemverwaltung: Hardware-Inventur	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Objekt der Hardware-Inventarisierung abrufen oder exportieren: **Lesen** • Objekt der Hardware-Inventarisierung hinzufügen, einstellen oder löschen: **Schreiben**	Nichts
Systemverwaltung: Network Access Control (NAC)	• **Lesen** • **Schreiben**	• CISCO-Einstellungen anzeigen: **Lesen** • CISCO-Einstellungen ändern: **Schreiben**	Nichts
Systemverwaltung: Bereitstellung des Betriebssystems	• **PXE-Server bereitstellen** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Bereitstellung von PXE-Servern: **PXE-Server bereitstellen** • Liste mit PXE-Servern anzeigen: **Lesen** • Installationsprozess auf PXE-Clients starten oder stoppen: **Ausführen** • Treiber für WinPE und andere Betriebssysteme verwalten: **Schreiben**	"Installationspaket a eines Referenzimag einem Betriebssyste erstellen"
Systemverwaltung: Schwachstellen- und Patch-Management	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Eigenschaften von Patches von Drittanbietern anzeigen: **Lesen** • Eigenschaften von Patches von Drittanbietern ändern: **Schreiben**	• "Windows-Upd synchronisierer • "Updates von W Update installie • "Schwachstelle schließen" • "Erforderliche U installieren und Schwachstellen schließen"
Systemverwaltung: Remote-Installation	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Anzeigen von Drittanbieter-Installationspaketen, die auf dem Schwachstellen- und Patch-Management basieren: **Lesen** • Ändern von Drittanbieter-Installationspaketen, die auf dem Schwachstellen- und Patch-Management basieren: **Schreiben**	Nichts
Systemverwaltung: Software-Inventur	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	Nichts	Nichts

Vorkonfigurierte Benutzerrollen

Benutzer von Kaspersky Security Center mit zugewiesenen Benutzerrollen bekommen Zugriffsrechte auf Programmfunktionen gewährt.

Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Sie können entweder vordefinierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen. Beim Erstellen einer neuen Rolle müssen Sie den Gültigkeitsbereich der Rolle festlegen und die Zugriffsberechtigungen auf die Funktionen von Kaspersky Security Center selbst zuweisen. Einige der in Kaspersky Security Center verfügbaren, vorkonfigurierten Rollen können entsprechenden beruflichen Positionen, wie bspw. **Auditor**, **Security Officer** oder **Supervisor** zugeordnet werden (Diese Rollen stehen in Kaspersky Security Center ab der Version 11 zur Verfügung). Die Zugriffsberechtigungen dieser Rollen wurden gemäß den Standardaufgaben und den Tätigkeitsbereichen der entsprechenden Positionen vorkonfiguriert. Die folgende Tabelle gibt an, wie Rollen mit spezifischen beruflichen Positionen verbunden werden können.

Beispiele von Rollen für spezifische berufliche Positionen

Rolle	Kommentar
Auditor	Erlaubt alle Anzeigevorgänge und die Ausführung aller erstellten Aufgaben auf ausgewählten Geräten, die mit dem Administrationsserver über den Administrationsagenten mit lokalen Administratorrechten (root für Linux) verbunden sind. Es wird empfohlen, diese Rolle umsichtig zu gewähren und nur einer begrenzten Anzahl von Benutzern zuzuweisen, die diese Rechte zur Erfüllung ihrer offiziellen Verpflichtungen benötigen.
Supervisor	Erlaubt alle Anzeige-Vorgänge, erlaubt keine anderen Vorgänge. Sie können diese Rolle einem Security Officer und anderen Verantwortlichen zuweisen, die für die IT-Sicherheit in Ihrer Organisation zuständig sind.
Security Officer	Erlaubt alle Anzeige-Vorgänge, erlaubt Berichtsverwaltung; gewährt eingeschränkte Beschränkungen im Bereich **Systemverwaltung**: **Konnektivität**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.

Die folgende Tabelle gibt die jeder vorkonfigurierten Benutzerrolle zugewiesenen Zugriffsberechtigungen an.

Zugriffsberechtigungen von vorkonfigurierten Benutzerrollen

Rolle	Beschreibung
Administrator des Administrationsserver	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verarbeitung von Ereignissen** • **Hierarchie des Administrationsservers** • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Konnektivität** • **Hardware-Inventarisierung** • **Software-Inventur** Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.
Operator des Administrationsserver	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Konnektivität** • **Hardware-Inventarisierung** • **Software-Inventur**

Rolle	Beschreibung
Auditor	Gewährt alle Vorgänge in den Funktionsbereichen in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Gelöschte Objekte** • **Erzwungene Berichtsverwaltung** Sie können diese Rolle einer Person zuweisen, die das Audit Ihres Unternehmens durchführt.
Installationsadministrator	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Kaspersky software deployment** • **Verwaltung von Lizenzschlüsseln** • **Systemverwaltung**: • **Bereitstellung des Betriebssystems** • **Schwachstellen- und Patch-Management** • **Remote-Installation** • **Software-Inventur** Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen: Virtuelle Administrationsserver**.
Installationsoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verteilung der Software von Kaspersky** (gewährt auch die Funktion **Verwaltung der Patches von Kaspersky** in diesem Bereich) • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Bereitstellung des Betriebssystems** • **Schwachstellen- und Patch-Management** • **Remote-Installation** • **Software-Inventur**
Administrator von Kaspersky Endpoint Security	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.
Operator von Kaspersky Endpoint Security	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security
Hauptadministrator	Gewährt alle Vorgänge in Funktionsbereichen, *außer* für die folgenden Bereiche in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung** Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.

Rolle	Beschreibung
Hauptoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Gelöschte Objekte** • **Vorgänge auf dem Administrationsserver** • **Bereitstellen von Kaspersky-Anwendungen** • **Virtuelle Administrationsserver** • **Verwaltung mobiler Geräte: Allgemein** • **Systemverwaltung**, inklusive aller Funktionen • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security
Administrator der Funktion "Verwaltung mobiler Geräte"	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • **Verwaltung mobiler Geräte: Allgemein**
Operator der Funktion "Verwaltung mobiler Geräte"	Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen**: **Grundlegende Funktionen**. Gewährt die Berechtigungen **Lesen** und **Nur Informationsbefehle an mobile Geräte senden** in den Funktionsbereichen **Verwaltung mobiler Geräte**: **Allgemein**.
Security Officer	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung** Gewährt die Berechtigungen **Lesen**, **Schreiben**, **Ausführen**, **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** und **Ausführen von Vorgängen für die Geräteauswahlen** im Funktionsbereich **Systemverwaltung: Verbindungen**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.
Benutzer des Self Service Portals	Erlaubt alle Vorgänge im Funktionsbereich **Verwaltung mobiler Geräte: Self Service Portal**. Diese Funktionen wird nur von Kaspersky Security Center 11 oder höher unterstützt.
Supervisor	Gewährt die Berechtigung **Lesen** in den Funktionsbereichen **Allgemeine Funktionen**: **Zugriff auf Objekte, unabhängig von ihren ACLs** und **Allgemeine Funktionen**: **Erzwungene Berichtsverwaltung**. Sie können diese Rolle einem Security Officer und anderen Verantwortlichen zuweisen, die für die IT-Sicherheit in Ihrer Organisation zuständig sind.
Administrator der Funktionen "Schwachstellen- und Patch-Management"	Erlaubt alle Vorgänge in den Funktionsbereichen **Allgemeine Funktionen**: **Grundlegende Funktionen** und **Systemverwaltung** (einschließlich aller Funktionen).
Operator der Funktionen "Schwachstellen- und Patch-Management"	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in den Funktionsbereichen **Allgemeine Funktionen**: **Grundlegende Funktionen** und **Systemverwaltung** (einschließlich aller Funktionen).

Benutzerrollen hinzufügen

Um eine Benutzerrolle hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.

3. Wählen Sie im Fenster "Eigenschaften des Administrationsservers" im Bereich **Abschnitte** die Option **Benutzerrollen** aus und klicken Sie auf **Hinzufügen**.

   Der Abschnitt **Benutzerrollen** ist verfügbar, wenn die Option **Abschnitte mit Sicherheitseinstellungen anzeigen** aktiviert ist.

4. Passen Sie im Eigenschaftenfenster **Neue Rolle** die Eigenschaften der Rolle an:

   - Wählen Sie unter **Abschnitte** den Punkt **Allgemein** und geben Sie den Namen der Rolle an.

     Der Name der Rolle darf nicht mehr als 100 Zeichen umfassen.

   - Wählen Sie den Abschnitt **Berechtigungen** aus und passen Sie die Auswahl der Berechtigungen an, indem Sie neben den Programmfunktionen die Kontrollkästchen **Zulassen** und **Verbieten** aktivieren.

   Wenn Sie auf dem primären Administrationsserver arbeiten, können Sie die Option **Liste der Rollen an sekundäre Administrationsserver weiterleiten** aktivieren.

5. Klicken Sie auf die Schaltfläche **OK**.

Die Rolle wurde hinzugefügt.

Die für den Administrationsserver erstellten Benutzerrollen werden im Eigenschaftenfenster des Servers im Abschnitt **Benutzerrollen** angezeigt. Sie können Benutzerrollen ändern und löschen sowie Rollen den Sicherheitsgruppen oder einzelnen Benutzers zuweisen.

Einem Benutzer oder einer Sicherheitsgruppe eine Rolle zuweisen

Gehen Sie wie folgt vor, um einem Benutzer oder einer Benutzergruppe eine Rolle zuzuweisen:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Sicherheit** aus.

   Der Abschnitt **Sicherheit** ist verfügbar, wenn im Fenster zur Anpassung der Benutzeroberfläche das Kontrollkästchen **Abschnitte mit Sicherheitseinstellungen anzeigen** aktiviert ist.

4. Wählen Sie im Feld **Gruppen- oder Benutzernamen** den Benutzer oder die Benutzergruppe aus, dem bzw. der die Rolle zugewiesen werden soll.

   Wenn im Feld kein Benutzer bzw. keine Benutzergruppe angegeben ist, fügen Sie diese mithilfe der Schaltfläche **Hinzufügen** hinzu.

   Beim Hinzufügen eines Benutzers mithilfe der Schaltfläche **Hinzufügen** kann die Art der Benutzerauthentifizierung (Microsoft Windows oder Kaspersky Security Center) gewählt werden. Die Authentifizierung mittels Kaspersky Security Center wird bei der Auswahl von Benutzerkonten für interne Benutzer verwendet, die für die Arbeit mit virtuellen Administrationsservern genutzt werden.

5. Wechseln Sie zur Registerkarte **Rollen** und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Benutzerrollen** wird geöffnet. In diesem Fenster werden die erstellten Benutzerrollen angezeigt.

6. Wählen Sie im Fenster **Benutzerrollen** die Rolle für die Sicherheitsgruppe aus.

7. Klicken Sie auf die Schaltfläche **OK**.

Als Ergebnis wird dem Benutzer bzw. der Sicherheitsgruppe die Rolle mit einer Auswahl von Berechtigungen für die Arbeit mit dem Administrationsserver zugewiesen. Die zugewiesenen Rollen werden im Eigenschaftenfenster des Administrationsservers auf der Registerkarte **Rollen** im Abschnitt **Sicherheit** angezeigt.

Zuweisen von Berechtigungen an Benutzer und Gruppen

Sie können Benutzern und Gruppen Berechtigungen zur Nutzung verschiedener Funktionen von Administrationsserver und der Programme von Kaspersky, für die Sie über Verwaltungs-Plug-ins verfügen, erteilen, beispielsweise Kaspersky Endpoint Security für Windows.

Gehen Sie wie folgt vor, um einem Benutzer oder einer Benutzergruppe Berechtigungen zuzuweisen:

1. Führen Sie in der Konsolenstruktur eine der folgenden Aktionen aus:

   - Erweitern Sie den Knoten **Administrationsserver** und wählen Sie den Unterordner mit dem Namen des gewünschten Administrationsservers aus
   - Wählen Sie die Administrationsgruppe aus

2. Wählen Sie im Kontextmenü des Administrationsservers oder der Administrationsgruppe **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers (oder im Eigenschaftenfenster der Administrationsgruppe), das sich daraufhin öffnet, im rechten Bereich **Abschnitte** die Option **Sicherheit** aus.

   Der Abschnitt **Sicherheit** ist verfügbar, wenn im Fenster zur Anpassung der Benutzeroberfläche das Kontrollkästchen **Abschnitte mit Sicherheitseinstellungen anzeigen** aktiviert ist.

4. Wählen Sie im Bereich **Sicherheit** in der Liste **Gruppen- oder Benutzernamen** einen Benutzer oder eine Gruppe aus.

5. Passen Sie in der Liste der Berechtigungen im unteren Bereich des Arbeitsbereichs auf der Registerkarte **Berechtigungen** den Satz der Rechte für den Benutzer oder die Gruppe an:

   a. Klicken Sie auf die Pluszeichen (+), um die Knoten in der Liste zu erweitern und Zugriff auf die Berechtigungen zu erhalten.

   b. Aktivieren Sie die Kontrollkästchen **Zulassen** und **Verbieten** neben den gewünschten Berechtigungen.

   Beispiel 1: Erweitern Sie entweder den Knoten **Auf Objekte unabhängig von ihren ACLs zugreifen** oder den Knoten **Gelöschte Objekte** und wählen Sie **Lesen** aus.

   Beispiel 2: Erweitern Sie den Knoten **Grundlegende Funktionen** und wählen Sie **Schreiben** aus.

6. Wenn Sie den Satz der Rechte angepasst haben, klicken Sie auf **Übernehmen**.

Der Satz der Rechte für den Benutzer oder die Benutzergruppe wird angepasst.

Die Berechtigungen des Administrationsservers (oder der Administrationsgruppe) sind in die folgenden Bereiche unterteilt:

- Allgemeine Funktionen:
  - Verwaltung von Administrationsgruppen
  - Zugriff auf Objekte, unabhängig von deren ACLs
  - Grundlegende Funktionen
  - Gelöschte Objekte
  - Verarbeitung von Ereignissen
  - Vorgänge mit dem Administrationsserver (nur im Eigenschaftenfenster von Administrationsserver)
  - Bereitstellung von Kaspersky-Anwendungen
  - Verwaltung von Lizenzschlüsseln
  - Erzwungene Berichtsverwaltung
  - Serverhierarchie
  - Benutzerrechte
  - Virtuelle Administrationsserver
- Verwaltung mobiler Geräte:
  - Allgemein
- Systemverwaltung:
  - Konnektivität
  - Hardware-Inventarisierung
  - Network Access Control
  - Bereitstellung für das Betriebssystem
  - Verwaltung von Schwachstellen und Patches
  - Remote-Installation
  - Software-Inventur

Wenn für eine Berechtigung weder **Zulassen** noch **Verbieten** ausgewählt ist, dann gilt die Berechtigung als *Nicht festgestellt*: sie wird verboten bis sie für den Benutzer ausdrücklich verboten oder erlaubt wird.

Die Rechte eines Benutzers sind die Summe aus Folgendem:

- Eigene Rechte des Benutzers
- Rechte aller Rollen, die diesem Benutzer zugewiesen sind
- Rechte aller Sicherheitsgruppen, zu denen der Benutzer gehört
- Rechte aller Rollen, die den Sicherheitsgruppen zugewiesen sind, zu denen der Benutzer gehört

Wenn zumindest einer dieser Sätze von Rechten für eine Berechtigung **Verbieten** aufweist, erhält der Benutzer diese Berechtigung nicht, selbst wenn sie in anderen Sätze erlaubt oder nicht festgestellt ist.

Ausdehnen von Benutzerrollen auf sekundäre Administrationsserver

Standardmäßig sind die Listen der Benutzerrollen des primären und der sekundären Administrationsserver voneinander unabhängig. Sie können die Anwendung so anpassen, dass die auf dem primären Administrationsserver erstellten Benutzerrollen automatisch auf alle sekundären Administrationsserver verteilt werden. Die Benutzerrollen können auch von einem sekundären Administrationsserver auf dessen eigene sekundäre Administrationsserver verteilt werden.

Um Benutzerrollen vom primären Administrationsserver auf die sekundären Administrationsserver zu verteilen:

1. Öffnen Sie das Programmhauptfenster.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Namen des Administrationsservers und wählen Sie im Kontextmenü **Eigenschaften** aus.
   - Wenn Sie eine aktive Richtlinie des Administrationsservers haben, klicken Sie im Arbeitsbereich im Ordner **Richtlinien** mit der rechten Maustaste auf diese Richtlinie und wählen Sie im Kontextmenü **Eigenschaften** aus.
3. Wählen Sie im Fenster "Eigenschaften des Administrationsservers" oder im Fenster mit den Richtlinieneinstellungen im Bereich **Abschnitte** die Option **Benutzerrollen** aus.

   Der Abschnitt **Benutzerrollen** ist verfügbar, wenn die Option **Abschnitte mit Sicherheitseinstellungen anzeigen** aktiviert ist.

4. Aktivieren Sie die Option **Liste der Rollen an sekundäre Administrationsserver weiterleiten**.
5. Klicken Sie auf die Schaltfläche **OK**.

   Die Anwendung kopiert die Benutzerrollen des primären Administrationsservers auf die sekundären Administrationsserver.

Wenn die Option **Liste der Rollen an sekundäre Administrationsserver weiterleiten** aktiviert ist und die Benutzerrollen verteilt werden, können sie auf dem sekundären Administrationsserver nicht geändert oder gelöscht werden. Wenn Sie auf dem primären Administrationsserver eine neue Rolle erstellen oder eine bestehende ändern, werden die Änderungen automatisch auf die sekundären Administrationsserver kopiert. Wenn Sie auf dem primären Administrationsserver eine Benutzerrolle löschen, verbleibt diese Rolle danach auf den sekundären Administrationsservern, kann aber geändert oder gelöscht werden.

Die Rollen, die vom primären Administrationsserver an die sekundären Administrationsserver weitergegeben werden, sind mit einem Schloss-Symbol (🔒) markiert. Diese Rollen können auf dem sekundären Administrationsserver nicht bearbeitet werden.

Wenn Sie eine Rolle auf dem primären Administrationsserver erstellen, während auf seinem sekundären Administrationsserver eine Rolle mit demselben Namen vorhanden ist, wird die neue Rolle auf den sekundären Administrationsserver kopiert und der Rollenname um einen Index erweitert, z. B. ~~1 oder ~~2 (der Index kann eine Zufallszahl sein).

Wenn Sie die Option **Liste der Rollen an sekundäre Administrationsserver weiterleiten** deaktivieren, verbleiben alle Benutzerrollen auf den sekundären Administrationsservern, werden dabei jedoch von jeder Rolle auf dem primären Administrationsserver unabhängig. Nachdem sie unabhängig wurden, können die Benutzerrollen auf den sekundären Administrationsservern geändert oder gelöscht werden.

Benutzer zum Gerätebesitzer bestimmen

Sie können einen Benutzer zum Gerätebesitzer bestimmen, um das Gerät unter diesem Benutzer zu "festigen". Sollte es erforderlich sein, bestimmte Aktionen mit dem Gerät auszuführen (beispielsweise ein Hardware-Update), kann der Administrator den Gerätebesitzer informieren und die Aktion mit ihm abstimmen.

Gehen Sie folgendermaßen vor, um einen Benutzer zum Geräteinhaber zu bestimmen:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
2. Wählen Sie Im Arbeitsbereich auf der Registerkarte **Geräte** das Gerät aus, für das ein Eigentümer bestimmt werden soll.
3. Wählen Sie im Kontextmenü des Geräts den Punkt **Eigenschaften** aus.
4. Wählen Sie im Eigenschaftenfenster des Gerätes **Systeminformationen** → **Sitzungen**.
5. Klicken Sie auf die Schaltfläche **Zuweisen** neben dem Feld **Gerätebesitzer**.
6. Wählen Sie im Fenster **Benutzer auswählen** den Benutzer aus, der zum Gerätebesitzer bestimmt werden soll, und klicken Sie auf die Schaltfläche **OK**.
7. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin wird der Gerätebesitzer bestimmt. Das Feld **Gerätebesitzer** enthält standardmäßig einen Wert aus Active Directory und wird bei jeder Abfrage von Active Directory aktualisiert. Sie können sich eine Liste der Gerätebesitzer im **Bericht über Gerätebesitzer** anzeigen lassen. Der Bericht kann mithilfe des Assistenten zur Erstellung von Berichten erstellt werden.

Nachrichten an die Benutzer versenden

Gehen Sie folgendermaßen vor, um E-Mail-Nachrichten an Benutzer zu versenden:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzers die Option **Per E-Mail benachrichtigen** aus.

3. Füllen Sie im Fenster **Nachricht an Benutzer** die erforderlichen Felder aus und klicken Sie auf die Schaltfläche **OK**.

Als Ergebnis wird eine Nachricht an die in den Eigenschaften des Benutzers angegebene E-Mail-Adresse gesendet.

Um eine SMS-Nachricht an den Benutzer zu versenden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

2. Wählen Sie im Kontextmenü des Benutzers die Option **Eine SMS-Nachricht senden** aus.

3. Füllen Sie im Fenster **SMS-Text** die erforderlichen Felder aus und klicken Sie auf die Schaltfläche **OK**.

Als Ergebnis wird eine Nachricht an das mobile Gerät des Benutzers gesendet, dessen Nummer in den Eigenschaften des Benutzers angegeben ist.

Liste der mobilen Geräte des Benutzers anzeigen

Um eine Liste der mobilen Geräte anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Benutzerkontos den Abschnitt **Mobile Geräte** aus.

Im Abschnitt **Mobile Geräte** werden eine Liste der mobilen Geräte des Benutzers sowie Informationen über die mobilen Geräte angezeigt. Durch Klicken auf die Schaltfläche **In Datei exportieren** kann die Liste der mobilen Geräte in einer Datei gespeichert werden.

Benutzerzertifikat installieren

Sie können für einen Benutzer drei Arten von Zertifikaten installieren:

- Allgemeine Zertifikate zur Identifikation des mobilen Geräts des Benutzers
- E-Mail-Zertifikate für die Einrichtung der Unternehmens-E-Mail auf dem mobilen Gerät des Benutzers
- VPN-Zertifikate für die Einrichtung eines virtuellen privaten Netzwerks auf dem mobilen Gerät des Benutzers

Gehen Sie wie folgt vor, um für einen Benutzer ein Zertifikat auszustellen und zu installieren:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** und wählen Sie ein Benutzerkonto aus.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Zertifikat installieren** aus.

Der Assistent für die Installation eines Zertifikats wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Als Ergebnis der Ausführung des Assistenten für die Installation eines Zertifikats wird ein Zertifikat für den Benutzer erstellt und installiert. Sie können die Liste der installierten Benutzerzertifikate anzeigen und sie in eine Datei exportieren.

Liste der für den Benutzer ausgestellten Zertifikate

Um eine Liste aller für den Benutzer ausgestellten Zertifikate anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Benutzerkontos den Abschnitt **Zertifikate** aus.

Im Abschnitt **Zertifikate** werden eine Liste der Zertifikate des Benutzers sowie Informationen zu den Zertifikaten angezeigt. Durch Klicken auf die Schaltfläche **In Datei exportieren** können Sie die Liste der Zertifikate in einer Datei speichern.

Über den Administrator des virtuellen Administrationsservers

Ein Administrator des Unternehmensnetzwerks, das über einen virtuellen Administrationsserver verwaltet wird, startet Kaspersky Security Center Web Console unter dem Benutzerkonto, das in diesem Fenster festgelegt ist, um die Details des Antiviren-Schutzes anzuzeigen.

Bei Bedarf können Sie mehrere Benutzerkonten für die Administratoren des virtuellen Servers anlegen.

Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Der Administrator des virtuellen Administrationsservers ist ein interner Benutzer von Kaspersky Security Center. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center.

Remote-Installation von Betriebssystemen und Programmen

Kaspersky Security Center ermöglicht das Erstellen und die Verteilung von Betriebssystem-Images auf Client-Geräten eines Netzwerks sowie die Remote-Installation von Programmen von Kaspersky oder anderen Software-Herstellern.

Um Betriebssystem-Images zu erstellen, installieren Sie auf dem Administrationsserver die Windows ADK-Bereitstellungs-Tools und Tools des Windows PE Add-on für das Windows ADK. Sie können ein Image von jeder Version des Windows-Betriebssystems erstellen, die den Anforderungen von Kaspersky Security Center entspricht.

Kaspersky Security Center unterstützt die 64-Bit-Versionen von Windows ADK und Windows PE nicht.

Betriebssystem-Images aufzeichnen

Kaspersky Security Center ermöglicht das Aufzeichnen von Betriebssystem-Images der Zielgeräte und die Übertragung der Images an den Administrationsserver. Die dadurch erstellten Betriebssystem-Images werden in einem freigegebenen Ordner auf dem Administrationsserver gespeichert. Das Erstellen eines Betriebssystem-Images eines Mustergeräts erfolgt mit der Aufgabe zum Erstellen eines Installationspakets.

Die Funktion zum Aufzeichnen eines Betriebssystem-Images weist folgende Besonderheiten auf:

- Es kann kein Betriebssystem-Image des Geräts erstellt werden, auf dem der Administrationsserver installiert wurde.
- Beim Erstellen eines Betriebssystem-Images werden die Einstellungen des Mustergeräts durch das Tool sysprep.exe zurückgesetzt. Wenn die Einstellungen eines Mustergeräts wiederhergestellt werden sollen, müssen Sie im Assistenten für das Erstellen von Betriebssystem-Images das Kontrollkästchen **Backup-Kopie des Gerätestatus speichern** aktivieren.
- Beim Erstellen des Images wird ein Neustart des Mustergeräts durchgeführt.

Bereitstellung von Betriebssystem-Images auf neuen Geräten

Sie können die erstellten Images zur Bereitstellung auf neue Geräte des Netzwerks verwenden, auf denen noch kein Betriebssystem installiert wurde. Dazu wird die Technologie Preboot eXecution Environment (PXE) verwendet. Sie können ein im Netzwerk befindliches Gerät auswählen, das als PXE-Server fungieren soll. Dieses Gerät muss folgende Voraussetzungen erfüllen:

- Auf dem Gerät muss der Administrationsagent installiert sein.
- Auf dem Gerät darf kein DHCP-Server laufen, da der PXE-Server dieselben Ports verwendet wie der DHCP-Server.
- Im Netzwerksegment, zu dem das Gerät gehört, dürfen keine anderen PXE-Server vorhanden sein.

Um ein Betriebssystem bereitzustellen, müssen die folgenden Bedingungen erfüllt sein:

- In dem Gerät muss eine Netzwerkkarte installiert sein.
- Das Gerät muss mit dem Netzwerk verbunden sein.
- Im BIOS des Geräts muss die Option, über das Netzwerk zu booten, ausgewählt sein.

Die Bereitstellung des Betriebssystems erfolgt in folgender Reihenfolge:

1. Das Client-Gerät stellt während seines Startvorgangs eine Verbindung mit dem PXE-Server her.
2. Das Client-Gerät bootet in die Windows Preinstallation Environment (WinPE).

   Um ein Gerät in die WinPE-Umgebung einzubinden, müssen Sie ggf. die Treiber für die WinPE-Umgebung anpassen.

3. Das Client-Gerät wird auf dem Administrationsserver registriert.

4. Der Administrator weist dem Client-Gerät ein Installationspaket mit dem Abbild des Betriebssystems zu.

   Der Administrator kann erforderliche Treiber zum Installationspaket mit dem Abbild des Betriebssystems hinzufügen. Der Administrator kann auch eine Konfigurationsdatei mit den Einstellungen für das Betriebssystem (Antwortdatei) angeben, die während der Installation übernommen werden sollen.

5. Es erfolgt die Bereitstellung des Betriebssystems auf dem Client-Gerät.

Der Administrator kann MAC-Adressen der noch nicht verbundenen Client-Geräte manuell angeben und das Installationspaket mit dem Image des Betriebssystems den Geräten zuweisen. Bei der Verbindung der Client-Geräte mit dem PXE-Server wird das Betriebssystem automatisch auf diesen Geräten installiert.

Bereitstellung von Betriebssystem-Images auf Geräten mit bereits installierten Betriebssystem

Die Bereitstellung von Betriebssystem-Images auf Client-Geräten mit bereits installierten Betriebssystem erfolgt mit einer Aufgabe zur Remote-Installation für eine Reihe von Geräten.

Beachten Sie, dass eine Neuinstallation des Betriebssystems durchgeführt wird. Dabei werden alle Daten gelöscht.

Kaspersky-Programme und Programme anderer Software-Hersteller installieren

Der Administrator kann für beliebige Programme, unter anderem für vom Benutzer angegebene Programme, Installationspakete erstellen und diese Programme mit einer Aufgabe zur Remote-Installation auf den Client-Geräten installieren.

Betriebssystem-Abbilder erstellen

Das Erstellen von Betriebssystem-Images erfolgt mit der Aufgabe zum Erfassen eines Betriebssystem-Images des Mustergeräts.

Gehen Sie wie folgt vor, um eine Aufgabe zum Erfassen eines Betriebssystem-Image anzulegen:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.

2. Starten Sie über den Link **Installationspaket erstellen** den Assistenten für das Erstellen eines Installationspakets.

3. Klicken Sie im Fenster des Assistenten **Typ des Installationspakets auswählen** auf die Schaltfläche **Installationspaket auf Basis eines Betriebssystem-Images erstellen**.

4. Folgen Sie den Anweisungen des Assistenten.

   Nach Abschluss des Assistenten wird die Aufgabe des Administrationsservers **Installationspaket anhand des Betriebssystem-Images des Mustergeräts erstellen** erstellt. Sie können sich die Aufgabe im Ordner **Aufgaben** anzeigen lassen.

Nach Fertigstellung der Aufgabe **Installationspaket anhand des Betriebssystem-Images des Mustergeräts erstellen** wird das Installationspaket erstellt, das Sie zur Bereitstellung für das Betriebssystem auf den Client-Geräten mithilfe eines PXE-Servers oder einer Aufgabe zur Remote-Installation verwenden können. Sie können das Installationspaket im Ordner **Installationspakete** ansehen.

Betriebssystem-Images installieren

Kaspersky Security Center erlaubt, auf den Geräten des Unternehmensnetzwerks wim-Images der Desktop- und Serverversionen des Betriebssystems Windows® zu verteilen.

Ein Betriebssystem-Image, das für die Bereitstellung mithilfe von Kaspersky Security Center geeignet ist, kann auf folgende Weisen erstellt werden:

- Durch Import aus der Datei install.wim, die zum Lieferumfang des Windows-Programmpakets gehört.
- Durch Aufzeichnen eines Images auf einem Standardgerät.

Es werden zwei Szenarien zur Bereitstellung des Betriebssystem-Images unterstützt:

- Bereitstellung auf ein "blankes" Gerät, das heißt auf ein Gerät ohne darauf installiertem Betriebssystem.
- Bereitstellung auf ein Gerät unter Verwaltung des Betriebssystems Windows.

Verwenden Sie die Windows Preinstallation Environment (Windows PE) zum Erfassen und Bereitstellen von Betriebssystem-Images. Zu WinPE müssen alle Treiber hinzugefügt werden, die für eine ordnungsgemäße Ausführung aller Geräte erforderlich sind. Im Allgemeinen müssen Treiber für die Netzwerkadapter und den Speicher-Controller hinzugefügt werden.

Für die Implementierung der Szenarien zur Bereitstellung und zum Aufzeichnen der Images müssen die folgenden Anforderungen erfüllt sein:

- Auf dem Administrationsserver muss das Windows Automated Installation Kit (WAIK) Version 2.0 oder höher oder Windows ADK mit dem Windows PE-Add-on für das Windows ADK installiert sein. Wenn dieses Szenario für die Installation oder die Erstellung von Images auf Windows XP vorgesehen ist, muss WAIK installiert werden.
- Im Netzwerk, in dem sich das Gerät befindet, muss ein DHCP-Server vorhanden sein.
- Der freigegebene Ordner des Administrationsservers muss über Leseberechtigung aus dem Netzwerk verfügen, in dem sich das Gerät befindet. Wenn sich der freigegebene Ordner auf dem Administrationsserver befindet, ist Zugang für das Benutzerkonto KlPxeUser erforderlich (dieses Benutzerkonto wird automatisch während der Ausführung des Installers des Administrationsservers erstellt). Wenn sich der Ordner außerhalb des Administrationsservers befindet, ist ein Zugriff für alle erforderlich.

Bei der Auswahl des Betriebssystem-Images für die Installation muss der Administrator die Prozessorarchitektur des Geräts explizit angeben: x86 oder x86-64.

Adresse von KSN-Proxyserver anpassen

Standardmäßig stimmt der Verbindungsname oder die IP-Adresse des Administrationsservers mit der Adresse des KSN-Proxyservers überein. Falls Sie den Verbindungsnamen oder die IP-Adresse des Administrationsservers ändern, müssen Sie die korrekte Adresse des KSN-Proxyservers angeben, um zu verhindern, dass die Verbindung zwischen Host-Geräten und KSN getrennt wird.

So konfigurieren Sie die Adresse des KSN-Proxyservers:

1. Wechseln Sie in der Konsolenstruktur zu **Erweitert** → **Remote-Installation** → **Installationspakete**.
2. Wählen Sie im Kontextmenü von **Installationspakete** den Punkt **Eigenschaften** aus.
3. Geben Sie im nächsten Fenster auf der Registerkarte **Allgemein** die neue Adresse des KSN-Proxyservers an.
4. Klicken Sie auf die Schaltfläche **Übernehmen**.

Ab jetzt wird die angegebene Adresse als Adresse des KSN-Proxyservers verwendet. Es wird empfohlen, dass Sie die Option **KSN-Proxy verwenden** verwenden, um den Datenverkehr in Ihrem Netzwerk zu optimieren.

Treiber für die Windows-Vorinstallationsumgebung (WinPE) hinzufügen

Um Treiber für die Windows-Vorinstallationsumgebung (WinPE) hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Remote-Installation** in der Konsolenstruktur den Unterordner **Geräte-Images verteilen** aus.
2. Klicken Sie im Arbeitsbereich des Ordners **Geräte-Images verteilen** auf die Schaltfläche **Weitere Aktionen** und wählen Sie in der Dropdown-Liste die Option **Treiber für die Windows-Vorinstallationsumgebung (WinPE) anpassen**.

   Das Fenster **Treiber für die Windows-Vorinstallationsumgebung** wird geöffnet.
3. Klicken Sie im Fenster **Treiber für die Windows-Vorinstallationsumgebung** auf **Hinzufügen**.

   Das Fenster **Treiber auswählen** wird geöffnet.
4. Wählen Sie im Fenster **Treiber auswählen** einen Treiber aus der Liste aus.

   Sollte der erforderliche Treiber in der Liste fehlen, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im folgenden Fenster **Treiber hinzufügen** den Treibernamen und den Ordner mit dem Treiber-Programmpaket an.

   Sie können den Ordner mithilfe der Schaltfläche **Durchsuchen** auswählen.

   Klicken Sie im Fenster **Treiber hinzufügen** auf **OK**.
5. Klicken Sie im Fenster **Treiber auswählen** auf **OK**.

   Der Treiber wird zur Datenverwaltung des Administrationsservers hinzugefügt. Der neu zur Datenverwaltung hinzugefügte Treiber wird im Fenster **Treiber auswählen** angezeigt.
6. Klicken Sie im Fenster **Treiber für die Windows-Vorinstallationsumgebung** auf **OK**.

Der Treiber wird zur Windows-Vorinstallationsumgebung (WinPE) hinzugefügt.

Treiber zum Installationspaket mit dem Betriebssystem-Abbild hinzufügen

Um Treiber zum Installationspaket mit dem Betriebssystem-Abbild hinzuzufügen, gehen Sie folgendermaßen vor.

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.
2. Klicken Sie mit der rechten Maustaste auf das Installationspaket mit dem Betriebssystem-Abbild und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Installationspakets wird geöffnet.
3. Wählen Sie im Eigenschaftenfenster des Installationspakets den Bereich **Zusätzliche Treiber**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen** im Abschnitt **Zusätzliche Treiber**.

   Das Fenster **Treiber auswählen** wird geöffnet.
5. Wählen Sie im Fenster **Treiber auswählen** die Treiber aus, die Sie zum Installationspaket des Betriebssystem-Abbildes hinzufügen möchten.

   Sie können neue Treiber zur Datenverwaltung des Administrationsservers hinzufügen, indem Sie auf die Schaltfläche **Hinzufügen** im Fenster **Treiber auswählen** klicken.
6. Klicken Sie auf die Schaltfläche **OK**.

Die neu hinzugefügten Treiber werden unter **Zusätzliche Treiber** im Eigenschaftenfenster des Installationspakets mit dem Betriebssystem-Abbild angezeigt.

Einstellungen des Tools sysprep.exe anpassen

Das Tool sysrep.exe wird für die Vorbereitung des Geräts auf das Erstellen seines Betriebssystemabbildes verwendet.

Um die Einstellungen für das Tool sysprep.exe anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.
2. Klicken Sie mit der rechten Maustaste auf das Installationspaket mit dem Betriebssystem-Abbild und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Installationspakets wird geöffnet.
3. Wählen Sie im Eigenschaftenfenster des Installationspakets den Bereich **Einstellungen für sysprep.exe**.

4. Geben Sie im Abschnitt **Einstellungen für Einstellungen für sysprep.exe** die Konfigurationsdatei an, die für die Bereitstellung für das Betriebssystem auf dem Client-Gerät verwendet werden soll:

   - **Standard-Konfigurationsdatei verwenden**. Wählen Sie diese Option, wenn Sie die Antwortdatei verwenden möchten, die standardmäßig bei der Aufzeichnung des Betriebssystem-Abbilds erstellt wird.
   - **Benutzerdefinierte Werte der wichtigsten Einstellungen festlegen**. Wählen Sie diese Option, um die Einstellungswerte anhand der Benutzeroberfläche festzulegen.
   - **Konfigurationsdatei angeben**. Wählen Sie diese Option, um eine eigene Konfigurationsdatei zu verwenden.

5. Klicken Sie auf die Schaltfläche **Übernehmen**, damit die vorgenommenen Änderungen wirksam werden.

Bereitstellung für Betriebssysteme auf neuen Geräte des Netzwerks

Gehen Sie wie folgt vor, um ein Betriebssystem auf neue Geräte zu verteilen, auf denen noch kein Betriebssystem installiert wurde:

1. Wählen Sie im Ordner **Remote-Installation** in der Konsolenstruktur den Unterordner **Geräte-Images verteilen** aus.

   Stellen Sie sicher, dass die Option **Schwachstellen- und Patch-Management anzeigen** im Fenster **Benutzeroberfläche anpassen** aktiviert ist. Andernfalls wird der Ordner **Remote-Installation** nicht angezeigt.

2. Klicken Sie auf die Schaltfläche **Weitere Aktionen** und wählen Sie **Liste der PXE-Server im Netzwerk verwalten** in der Dropdown-Liste.

   Dieser Link öffnet das Fenster **Eigenschaften**: **Geräten-Images verteilen** mit dem Abschnitt **PXE-Server**.

3. Klicken Sie im Abschnitt **PXE-Server** auf die Schaltfläche **Hinzufügen** und wählen Sie im folgenden Fenster **PXE-Server** das Gerät aus, das als PXE-Server verwendet werden soll.

   Das hinzugefügte Gerät wird im Abschnitt PXE-Server angezeigt. Die erstellten WinPE-Dateien werden vom Administrationsserver auf das Gerät übertragen. Die Datenübertragung dauert normalerweise 10 Minuten. Nach Abschluss der Übertragung ändert sich der angezeigte Wert **Status** von **Erste Schritte** auf **Fertig**.

4. Wählen Sie im Abschnitt **PXE-Server** den PXE-Server aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.

5. Passen Sie im Eigenschaftenfenster des gewählten PXE-Servers im Abschnitt **Einstellungen für die Verbindung zum PXE-Server** die Einstellungen für die Verbindung des Administrationsservers mit dem PXE-Server an.

6. Starten Sie das Client-Gerät, auf dem Sie das Betriebssystem installieren möchten.

7. Wählen Sie in der BIOS-Umgebung des Client-Geräts die Installationsvariante Netzwerkstart aus.

   Das Client-Gerät wird mit dem PXE-Server verbunden und im Arbeitsbereich des Ordners **Geräte-Images verteilen** angezeigt.

8. Wählen Sie im Abschnitt **Aktionen** durch Klicken auf den Link **Installationspaket bestimmen** das Installationspaket aus, das für die Installation des Betriebssystems auf dem gewählten Gerät verwendet werden soll.

   Verwenden Sie das Tool "DiskPart" auf dem ausgewählten Gerät, um die verfügbaren Datenträger zu überprüfen. Geben Sie in der Windows PE-Eingabeaufforderung `diskpart` ein, um das DiskPart-Tool zu öffnen. Geben Sie `list disk` ein, um die Laufwerke aufzulisten.

Sobald das Gerät hinzugefügt und ein Installationspaket dafür bestimmt wurde, beginnt die Bereitstellung für das Betriebssystem auf diesem Gerät automatisch.

9. Um die Bereitstellung für das Betriebssystem auf dem Client-Gerät abzubrechen, klicken Sie im Abschnitt **Aktionen** auf den Link **Installation von Betriebssystem-Abbildern abbrechen**.

Um ein Gerät nach seiner MAC-Adresse hinzuzufügen:

- Klicken Sie im Ordner **Geräte-Images verteilen** auf den Link **MAC-Adresse eines Geräts hinzufügen** und geben Sie im folgenden Fenster **Neues Gerät** die MAC-Adresse des Geräts an, das Sie hinzufügen möchten.

- Wählen Sie durch Klicken auf den Link **Geräte-Images verteilen** im Ordner **MAC-Adressen der Geräte aus Datei importieren** die Datei aus, welche die Liste der MAC-Adressen aller Geräte enthält, auf denen Sie das Betriebssystem installieren möchten.

Bereitstellung für Betriebssysteme auf Client-Geräten

Gehen Sie wie folgt vor, um ein Betriebssystem auf Client-Geräten bereitzustellen, auf denen ein Betriebssystem bereits installiert ist:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Remote-Installation** und klicken Sie den Link **Installationspakete auf den verwalteten Geräten (Workstations) bereitstellen**, um den Assistenten für die Bereitstellung des Schutzes zu starten.

2. Geben Sie im Fenster des Assistenten **Installationspaket auswählen** das Installationspaket mit dem Betriebssystem-Abbild an.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe zur Remote-Installation des Betriebssystems auf Client-Geräten erstellt. Sie können die Aufgabe im Ordner **Aufgaben** starten oder beenden.

Installationspakete für Programme erstellen

Gehen Sie wie folgt vor, um ein Installationspaket für ein Programm zu erstellen:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.

2. Starten Sie über den Link **Installationspaket erstellen** den Assistenten für das Erstellen eines Installationspakets.

3. Klicken Sie im Fenster des Assistenten **Typ des Installationspakets auswählen** auf eine der folgenden Schaltflächen:

   - **Installationspaket für ein Programm von Kaspersky erstellen**. Wählen Sie diese Option aus, wenn Sie das Installationspaket für eine Kaspersky-Anwendung erstellen möchten.

   - **Installationspaket für eine angegebene ausführbare Datei erstellen**. Wählen Sie diese Option aus, wenn Sie das Installationspaket für ein Drittanbieter-Programm mithilfe einer ausführbaren Datei erstellen möchten. In der Regel ist die ausführbare Datei eine Setup-Datei des Programms.

     - **Den gesamten Ordner ins Installationspaket kopieren**

       Wählen Sie diese Option, wenn zur ausführbaren Datei noch zusätzliche Dateien gehören, die für die Programminstallation benötigt werden. Bevor Sie diese Option aktivieren, stellen Sie sicher, dass alle erforderlichen Dateien im selben Ordner gespeichert sind. Wenn diese Option aktiviert ist, fügt das Programm den gesamten Inhalt des Ordners, einschließlich der angegebenen ausführbaren Datei, zum Installationspaket hinzu.

     - **Installationsparameter angeben**

       Damit die Remote-Installation erfolgreich verläuft, müssen die meisten Programme im Silent-Modus installiert werden. Wenn dies der Fall ist, müssen Sie Parameter für die Installation im Silent-Modus angeben.

       Konfigurieren Sie die Installationseinstellungen:

       - **Befehlszeilenparameter der ausführbaren Datei**

         Wenn das Programm zusätzliche Parameter für eine Installation im Silent-Modus erfordert, geben Sie diese in diesem Feld an. Weitere Informationen finden Sie in der Dokumentation des Herstellers.

         Sie können auch andere Parameter angeben.

       - **Einstellungen auf die empfohlene Werte der von Kaspersky Security Center erkannte Programme konvertieren**

         Das Programm wird mit den empfohlenen Einstellungen installiert, wenn die Kaspersky-Datenbank Informationen zum entsprechenden Programm enthält.

         Wenn Sie Parameter im Feld **Befehlszeilenparameter der ausführbaren Datei** eingegeben haben, werden sie mit den empfohlenen Einstellungen überschrieben.

         Diese Option ist standardmäßig aktiviert.

         Die Kaspersky-Datenbank wird von den Analysten von Kaspersky erstellt und gepflegt. Für jedes Programm, das zur Datenbank hinzugefügt wird, definieren die Analysten von Kaspersky die optimalen Installationseinstellungen. Die Einstellungen werden so gewählt, dass eine erfolgreiche Remote-Installation des Programms auf einem Client-Gerät gewährleistet wird. Die Datenbank wird automatisch auf dem Administrationsserver aktualisiert, wenn Sie die Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers starten.

   - **Installationspaket für ein ausgewähltes Programm aus der Kaspersky-Datenbank erstellen**. Wählen Sie diese Option aus, wenn Sie das gewünschte Drittanbieter-Programm, für das ein Installationspaket erstellt werden soll, aus der Kaspersky-Datenbank wählen möchten. Die Datenbank wird automatisch erstellt, wenn Sie die Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers starten; Die Programme werden in der Liste angezeigt.

- **Installationspaket auf Basis eines Betriebssystem-Images erstellen**. Wählen Sie diese Option aus, wenn Sie das Installationspaket mit dem Betriebssystem-Abbild eines Mustergeräts erstellen möchten.

  Nach Abschluss des Assistenten wird eine Aufgabe des Administrationsservers mit dem Namen **Installationspaket anhand des Betriebssystem-Images des Mustergeräts erstellen** erstellt. Nach Fertigstellung der Aufgabe wird ein Installationspaket erstellt, das zur Bereitstellung für das Betriebssystem-Image mithilfe eines PXE-Servers oder einer Aufgabe zur Remote-Installation verwendet werden kann.

4. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird ein Installationspaket erstellt, das für die Installation des Programms auf den Client-Geräten verwendet werden kann. Wählen Sie in der Konsolenstruktur **Installationspakete** aus, um die Installationspakete anzuzeigen.

Ausgabe eines Zertifikats für Installationspakete von Programmen

Gehen Sie wie folgt vor, um ein Zertifikat für ein Installationspaket eines Programms auszustellen:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.

   Der Ordner **Remote-Installation** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Wählen Sie im Kontextmenü des Ordners **Installationspakete** den Punkt **Erweitert** aus.

   Daraufhin wird das Eigenschaftenfenster des Ordners **Installationspakete** geöffnet.

3. Wählen Sie im Eigenschaftenfenster **Installationspakete** den Abschnitt **Signatur der autonomen Pakete**.

4. Klicken Sie im Abschnitt **Signatur der autonomen Pakete** auf die Schaltfläche **Angeben**.

   Das Fenster **Zertifikat**.

5. Wählen Sie im Feld **Zertifikatstyp** entweder einen offenen oder geschlossenen Zertifikatstyp aus:

   - Wenn der Wert **Container PKCS#12** ausgewählt ist, geben Sie die Zertifikatsdatei und das Kennwort an.
   - Wenn der Wert **X.509-Zertifikat** ausgewählt ist:

     a. Geben Sie die Datei des privaten Schlüssels an (Datei mit der Erweiterung *prk oder *.pem).

     b. Geben Sie das Kennwort des privaten Schlüssels an.

     c. Geben Sie die Datei des öffentlichen Schlüssels an (Datei mit der Erweiterung cer).

6. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin wird ein Zertifikat für das Installationspaket des Programms ausgestellt.

Programme auf Client-Geräten installieren

Gehen Sie wie folgt vor, um ein Programm auf Client-Geräten zu installieren:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Remote-Installation** und klicken Sie den Link **Installationspakete auf den verwalteten Geräten (Workstations) bereitstellen**, um den Assistenten für die Bereitstellung des Schutzes zu starten.

2. Geben Sie im Fenster des Assistenten **Installationspaket auswählen** das Installationspaket für das Programm an, das Sie installieren möchten.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe zur Remote-Installation des Programms auf den Client-Geräten angelegt. Sie können die Aufgabe im Ordner **Aufgaben** starten oder beenden.

Mithilfe des "Assistenten für die Bereitstellung des Schutzes" können Sie den Administrationsagenten auf Client-Geräten mit den Betriebssystemen Windows, Linux und macOS installieren.

Um die 64-Bit-Sicherheitsanwendungen auf Geräten mit den Betriebssystemen Linux mithilfe von Kaspersky Security Center zu verwalten, muss der 64-Bit-Administrationsagent für Linux verwendet werden. Sie können die benötigte Version des Administrationsagenten von der Webseite des Technischen Supports herunterladen.

Vor dem Ausführen der Remote-Installation des Administrationsagenten auf einem Gerät mit dem Betriebssystem Linux muss das Gerät vorbereitet werden.

Umgang mit Objekt-Revisionen

Der Abschnitt enthält Informationen über die Arbeit mit den Revisionen des Objekts. Kaspersky Security Center erlaubt eine Nachverfolgung der Änderungen von Objekten. Jedes Mal, wenn Sie die Änderungen des Objektes speichern, wird eine *Revision* erstellt. Jede Revision hat eine Nummer.

Folgende Objekte der Anwendung unterstützen die Arbeit mit Revisionen:

- Eigenschaften des Administrationsservers
- Richtlinien
- Aufgaben
- Administrationsgruppen
- Benutzerkonten
- Installationspakete

Sie können mit den Revisionen von Objekten folgende Aktionen ausführen:

- Ausgewählte Revisionen mit der laufenden Revision vergleichen
- Ausgewählte Revisionen vergleichen
- Objekt mit der ausgewählten Revision eines anderen gleichartigen Objekts vergleichen
- Ausgewählte Revision anzeigen
- Rollback der Änderungen des Objektes auf die ausgewählte Revision durchführen
- Revisionen in eine Datei im txt-Format speichern

Im Eigenschaftenfenster der Objekte, die Revisionen unterstützen, wird im Abschnitt **Revisionsverlauf** eine Liste der Objektrevisionen mit den folgenden Informationen angezeigt:

- Nummer der Revision des Objekts
- Datum und Uhrzeit der Objektänderung
- Name des Benutzers, der das Objekt geändert hat
- Ausgeführte Aktion mit dem Objekt
- Beschreibung der Revision der Änderungen der Objekteinstellungen

Über Objekt-Revisionen

Sie können mit den Revisionen von Objekten folgende Aktionen ausführen:

- Ausgewählte Revisionen mit der laufenden Revision vergleichen
- Ausgewählte Revisionen vergleichen
- Objekt mit der ausgewählten Revision eines anderen gleichartigen Objekts vergleichen
- Ausgewählte Revision anzeigen
- Rollback der Änderungen des Objektes auf die ausgewählte Revision durchführen
- Revisionen in eine Datei im txt-Format speichern

Im Eigenschaftenfenster der Objekte, die Revisionen unterstützen, wird im Abschnitt **Revisionsverlauf** eine Liste der Objektrevisionen mit den folgenden Informationen angezeigt:

- Nummer der Revision des Objekts
- Datum und Uhrzeit der Objektänderung
- Name des Benutzers, der das Objekt geändert hat

- Ausgeführte Aktion mit dem Objekt
- Beschreibung der Revision der Änderungen der Objekteinstellungen

Anzeigen des Abschnitts "Revisionsverlauf"

Sie können Revisionen des Objektes mit der aktuellen Revision vergleichen, Revisionen vergleichen, die in der Liste ausgewählt sind, oder eine Revision des Objekts mit der Revision eines anderen, gleichartigen Objekts vergleichen.

*Um Bereich **Revisionsverlauf** eines Objekts anzuzeigen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum eines der Objekte aus:
   - Knoten **Administrationsserver**
   - Ordner **Richtlinien**
   - Ordner **Aufgaben**
   - Ordner einer Administrationsgruppe
   - Ordner **Benutzerkonten**
   - Ordner **Gelöschte Objekte**
   - Unterordner **Installationspakete**, der sich im Ordner **Remote-Installation** befindet
2. Abhängig vom Ort des betreffenden Objekts führen Sie eine der folgenden Aktionen aus:
   - Wenn sich das Objekt im Knoten **Administrationsserver** oder dem Knoten einer Administrationsgruppe befindet, klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie im Kontextmenü **Eigenschaften** aus.
   - Wenn sich das Objekt in den Ordnern **Richtlinien**, **Aufgaben**, **Benutzerkonten**, **Gelöschte Objekte**, oder **Installationspakete** befindet, wählen Sie den Ordner und im entsprechenden Arbeitsbereich das Objekt aus.

   Daraufhin wird das Eigenschaftenfenster des Objekts geöffnet.
3. Wählen Sie im linken Bereich von **Abschnitte** die Option **Revisionsverlauf** aus.

   Daraufhin wird der Revisionsverlauf im Arbeitsbereich angezeigt.

Vergleich der Revisionen des Objekts

Sie können frühere Revisionen des Objektes mit der aktuellen Revision vergleichen, Revisionen vergleichen, die in der Liste ausgewählt sind, oder eine Revision des Objekts mit der Revision eines anderen, gleichartigen Objekts vergleichen.

Um Revisionen des Objekts zu vergleichen, gehen Sie wie folgt vor:

1. Wählen Sie ein Objekt aus und gehen Sie weiter zum Eigenschaftenfenster des Objekts.
2. Wechseln Sie im Eigenschaftenfenster zum Abschnitt **Revisionsverlauf**.
3. Wählen Sie im Arbeitsbereich in der Liste der Revisionen des Objekts die Revision für den Vergleich aus.

   Verwenden Sie für die Auswahl von mehr als einer Revision des Objekts die Tasten **`Umschalt`** und **`Strg`**.
4. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf die unterteilte Schaltfläche **Vergleichen** und wählen Sie in der Dropdown-Liste einen der folgenden Werte aus:

     - **Mit aktueller Revision vergleichen**

       Wählen Sie diese Variante aus, um die ausgewählte Revision mit der aktuellen zu vergleichen.

     - **Ausgewählte Revisionen vergleichen**

       Wählen Sie diese Variante aus, um zwei ausgewählte Revisionen zu vergleichen.

     - **Mit anderer Aufgabe vergleichen**

       Bei der Arbeit mit Revisionen von Aufgaben wählen Sie die Variante **Mit anderer Aufgabe vergleichen** aus, um die ausgewählte Revision mit der Revision einer anderen Aufgabe zu vergleichen.

       Bei der Arbeit mit Revisionen von Richtlinien wählen Sie die Variante **Mit anderer Richtlinie vergleichen** aus, um die ausgewählte Revision mit der Revision einer anderen Richtlinie zu vergleichen.

   - Doppelklicken Sie auf den Namen einer Revision und klicken Sie im nächsten Eigenschaftenfenster der Revision auf eine der folgenden Schaltflächen:

     - **Mit aktuellem vergleichen**

       Klicken Sie auf diese Schaltfläche, um die ausgewählte Revision mit der aktuellen Revision zu vergleichen.

     - **Mit vorhergehendem vergleichen**

       Klicken Sie auf diese Schaltfläche, um die ausgewählte Revision mit der vorhergehenden Revision zu vergleichen.

   Ein Bericht über den Vergleich der Revisionen wird im HTML-Format in Ihrem Standard-Browser angezeigt.

   Im Bericht können einige Einstellungsblöcke der Revision minimiert werden. Um einen Einstellungsblock der Revision zu minimieren, klicken Sie auf das Pfeil-Symbol (▲) neben dem Namen des Abschnitts.

Eine Revision des Administrationsservers enthält alle Details über durchgeführte Änderungen mit Ausnahme von Details aus den folgenden Bereichen:

- Bereich **Datenverkehr**
- Bereich **Regeln zur Zuweisung von Tags**
- Bereich **Benachrichtigung**
- Bereich **Verteilungspunkte**

- Bereich **Virenangriff**

  Aus dem Abschnitt **Virenangriff** werden keine Informationen über die Konfigurationsdatei für die Richtlinienaktivierung aufgezeichnet, die erfolgt, wenn ein Ereignis zu einem Virenangriff ausgelöst wird.

Sie können Revisionen eines gelöschten Objekts mit einer Revision eines bestehenden Objekts vergleichen, jedoch nicht umgekehrt: Sie können Revisionen eines bestehenden Objekts nicht mit einer Revision eines gelöschten Objekts vergleichen.

Einrichten der Speicherdauer für Revision des Objekts und für Information über gelöschte Objekte

Die Speicherdauer ist für Revision des Objekts und für Informationen über gelöschte Informationen gleich. Standardmäßig beträgt die Speicherdauer 90 Tage. Das ist ausreichend Zeit für das regelmäßige Audit des Programms.

Nur Benutzer mit Berechtigungen zum **Ändern** im Bereich **Gelöschte Objekte** können die Speicherdauer ändern.

Um die Speicherdauer für Revision des Objekts und für Informationen über gelöschte Informationen zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den Sie die Speicherdauer ändern möchten.
2. Drücken Sie die rechte Maustaste und wählen Sie im Kontextmenü **Eigenschaften** aus.
3. Geben Sie im folgenden Administrationsserver-Eigenschaftenfenster im Abschnitt **Datenverwaltung des Revisionsverlaufs** die gewünschte Speicherdauer an (Anzahl an Tagen).
4. Klicken Sie auf die Schaltfläche **OK**.

Die Revisionen des Objekts und Informationen über gelöschte Objekte werden für die eingegebene Anzahl an Tagen gespeichert.

Anzeigen der Revision des Objekts

Wenn es erforderlich ist, dass Sie erfahren, welche Änderungen in einem bestimmten Zeitraum an einem Objekt durchgeführt wurden, können Sie die Revisionen des Objekts anzeigen.

Um Revision des Objekts anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Abschnitt **Revisionsverlauf** des Objekts.
2. Wählen Sie in der Liste der Revisionen des Objektes die Revision aus, deren Einstellungen angezeigt werden sollen.

3. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Revision anzeigen**.
   - Öffnen Sie durch Doppelklick auf den Namen der Revision oder durch Klicken auf die Schaltfläche **Revision anzeigen** das Eigenschaftenfenster der Revision.

   Es wird ein Bericht mit den Einstellungen der ausgewählten Revision des Objektes im html-Format angezeigt. Im Bericht können einige Einstellungsblöcke der Revision des Objektes minimiert werden. Um einen Einstellungsblock der Revision zu minimieren, klicken Sie auf das Pfeil-Symbol (▲) neben dem Namen des Abschnitts.

Speichern der Revision des Objektes in einer Datei

Sie können die Revision des Objektes in einer Textdatei speichern, beispielsweise um die Datei per E-Mail zu versenden.

Um die Revision des Objektes in einer Datei zu speichern, gehen Sie wie folgt vor:

1. Wechseln Sie zum Abschnitt **Revisionsverlauf** des Objekts.
2. Wählen Sie in der Liste der Revisionen des Objektes die Revision aus, deren Einstellungen gespeichert werden sollen.
3. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **In Datei speichern**.

   Die Revision wird in einer Datei im txt-Format gespeichert.

Rollback der Änderungen

Falls erforderlich können Sie ein Rollback der Änderungen des Objekts durchführen. Beispielsweise kann es erforderlich sein, die Einstellungen der Richtlinie auf den Zustand eines bestimmten Datums zurückzusetzen.

Um ein Rollback der Änderungen einer Aufgabe durchzuführen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Abschnitt **Revisionsverlauf** des Objekts.
2. Wählen Sie in der Liste mit den Revisionen des Objekts die Nummer der Revision aus, auf deren Stand die Änderungen zurückgesetzt werden sollen.
3. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Rollback**.

   Es wird ein Rollback auf die ausgewählte Revision durchgeführt. In der Liste der Revisionen des Objektes wird ein Eintrag über die ausgeführte Aktion angezeigt. In der Beschreibung der Revision werden die Informationen über die Nummer der Revision angezeigt, auf die Sie das Objekt zurückgesetzt haben.

Hinzufügen einer Beschreibung der Revision

Sie können eine Beschreibung für die Revision hinzufügen, damit es künftiger einfacher ist, die gewünschte Revision in der Liste zu finden.

Um eine Beschreibung der Revision hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Abschnitt **Revisionsverlauf** des Objekts.
2. Wählen Sie in der Liste der Revisionen des Objektes die Revision aus, für die eine Beschreibung hinzugefügt werden soll.
3. Klicken Sie auf die Schaltfläche **Beschreibung**.
4. Geben Sie im Fenster **Beschreibung der Revision des Objekts** einen Text zur Beschreibung der Revision ein.

   Standardmäßig ist die Beschreibung der Revision des Objekts nicht ausgefüllt.
5. Klicken Sie auf die Schaltfläche **OK**.

Löschen von Objekten

Dieser Abschnitt enthält Informationen über das Löschen von Objekten.

Sie können Objekte löschen, einschließlich der folgenden:

- Richtlinien
- Aufgaben
- Installationspakete
- Virtuelle Administrationsserver
- Benutzer
- Sicherheitsgruppen
- Administrationsgruppen

Um ein Objekt zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie den erforderlichen Bereich in der Kaspersky Security Center Web Console und wählen Sie anschließend das Objekt aus.
2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Löschen**.
3. Klicken Sie im folgenden Fenster auf **OK**, um die Auswahl zu bestätigen.

   Das ausgewählte Objekt wird gelöscht.

Wenn Sie ein Objekt löschen, verbleiben die Informationen darüber in der Datenbank. Die Speicherdauer für Informationen über die gelöschten Objekte ist dieselbe wie die Speicherdauer für Revisionen des Objekts (die empfohlenen Dauer beträgt 90 Tage). Sie können die Speicherdauer nur ändern, wenn Sie über die Berechtigung **zum Ändern** im Berechtigungsbereich **Gelöschte Objekte** verfügen.

Über das Löschen von Client-Geräten

Wenn Sie ein verwaltetes Gerät aus einer Administrationsgruppe löschen, verschiebt die Anwendung das Gerät in die Gruppe "Nicht zugeordnete Geräte". Nach dem Löschen des Geräts verbleiben der installierte Administrationsagent und die Kaspersky-Sicherheitsanwendungen, wie Kaspersky Endpoint Security, auf dem Gerät.

Kaspersky Security Center geht mit den Geräten in der Gruppe "Nicht zugeordnete Geräte" gemäß den folgenden Regeln um:

- Wenn Sie Verschiebungsregeln für Geräte konfiguriert haben und ein Gerät die Kriterien einer Verschiebungsregel erfüllt, wird das Gerät automatisch gemäß dieser Regel in eine Administrationsgruppe verschoben.

- Das Gerät wird in der Gruppe "Nicht zugeordnete Geräte" gespeichert und entsprechend der Aufbewahrungsregeln für Geräte automatisch aus der Gruppe entfernt.

  Die Aufbewahrungsregeln für Geräte wirken sich nicht auf Geräte aus, in denen Laufwerke mit vollständiger Festplattenverschlüsselung verschlüsselt sind. Solche Geräte werden nicht automatisch gelöscht, sondern können nur manuell gelöscht werden. Wenn Sie ein Gerät mit einem verschlüsselten Laufwerk löschen müssen, entschlüsseln Sie zuerst das Laufwerk und löschen Sie anschließend das Gerät.

  > Wenn Sie ein Gerät mit einem verschlüsselten Laufwerk löschen, werden auch die zum Entschlüsseln des Laufwerks erforderlichen Daten gelöscht. Wenn Sie im Bestätigungsfenster, das sich öffnet, wenn Sie solche Geräte löschen (entweder aus der Gruppe **Nicht zugeordnete Geräte** oder aus der Gruppe **Verwaltete Geräte**), das Kontrollkästchen **Ich kenne das Risiko und möchte die ausgewählten Geräte löschen** aktivieren, geben Sie an, dass Sie von der anschließenden Datenlöschung Kenntnis haben.

  Um das Laufwerk zu entschlüsseln, müssen die folgenden Bedingungen erfüllt sein:

  - Das Gerät wird erneut mit dem Administrationsserver verbunden, um die zum Entschlüsseln des Laufwerks erforderlichen Daten wiederherzustellen.

  - Der Benutzer des Geräts merkt sich das Kennwort zum Entschlüsseln.

  - Die Sicherheitsanwendung, mit der das Laufwerk verschlüsselt wurde (z. B. Kaspersky Endpoint Security für Windows), ist weiterhin auf dem Gerät installiert.

  Wenn das Laufwerk mittels Kaspersky-Festplattenverschlüsselung verschlüsselt wurde, können Sie auch versuchen, die Daten mithilfe des Wiederherstellungs-Tools FDERT wiederherzustellen.

> Wenn Sie ein Gerät mit verschlüsselten Laufwerken in einer VDI-Umgebung besitzen, werden die Informationen auf dem verschlüsselten Laufwerk gelöscht, nachdem Sie das Gerät gelöscht haben.

Wenn Sie ein Gerät manuell aus der Gruppe "Nicht zugeordnete Geräte" löschen, entfernt die Anwendung das Gerät aus der Liste. Nach dem Löschen des Geräts verbleiben etwaige installierte Kaspersky -Anwendungen auf dem Gerät. Wenn das Gerät für den Administrationsserver weiterhin sichtbar ist und Sie die regelmäßige Netzwerkabfrage konfiguriert haben, erkennt Kaspersky Security Center das Gerät während der Netzwerkabfrage und fügt es erneut der Gruppe "Nicht zugeordnete Geräte" hinzu. Daher ist es sinnvoll, ein Gerät nur dann manuell zu löschen, wenn es für den Administrationsserver unsichtbar ist.

Löschen eines Objekts

Sie können Objekte wie Richtlinien, Aufgaben, Installationspakete, interne Benutzer und interne Sicherheitsgruppen löschen, wenn Sie über die Berechtigung "Ändern" in der Kategorie "Grundlegende Funktionen" von Berechtigungen verfügen (Weitere Informationen finden Sie unter Zuweisen von Berechtigungen an Benutzer und Gruppen).

> Sie können keine Installationspakete löschen, die im Rahmen von Aufgaben zur Remote-Installation verwendet werden. Bevor Sie dies möglich ist, müssen Sie zunächst die entsprechenden Aufgaben stoppen. Weitere Informationen über Aufgaben zur automatischen Installation einer innerhalb einer Administrationsgruppe finden Sie in diesem Artikel: Programme automatisch auf Geräten einer Administrationsgruppe installieren.

Um ein Objekt zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Arbeitsbereich des gewünschten Ordners ein Objekt aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Löschen** aus.
   - Drücken Sie die Taste **`Entf`**.

   Das Objekt wird gelöscht und die Informationen darüber werden in der Datenbank gespeichert.

Anzeigen von Informationen über gelöschte Objekte

Informationen über gelöschte Objekte werden im Ordner **Gelöschte Objekte** für dieselbe Zeitdauer gespeichert wie Revisionen des Objekts (die empfohlene Dauer beträgt 90 Tage).

Nur Benutzer mit der Berechtigung **Lesen** im Berechtigungsbereich **Gelöschte Objekte** können die Liste der gelöschten Objekte anzeigen (weitere Informationen finden Sie unter Zuweisen von Berechtigungen an Benutzer und Gruppen).

Um die Liste der gelöschten Objekte anzuzeigen, gehen Sie wie folgt vor:

Wählen Sie in der Konsolenstruktur **Gelöschte Objekte** aus (standardmäßig ist **Gelöschte Objekte** ein Unterordner von **Erweitert**).

Wenn Sie für den Berechtigungsbereich **Gelöschte Objekte** über keine Leseberechtigung verfügen, wird im Ordner **Gelöschte Objekte** eine leere Liste angezeigt.

Der Arbeitsbereich des Ordners **Gelöschte Objekte** enthält die folgenden Informationen über gelöschte Objekte:

- **Name**. Der Name des Objekts.
- **Typ**. Objekttyp, etwa Richtlinie, Aufgabe oder Installationspaket.
- **Uhrzeit**. Uhrzeit, zu der das Objekt gelöscht wurde.
- **Benutzer**. Benutzerkonto-Name des Benutzers, der das Objekt gelöscht hat.

Um Informationen über ein Objekt anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur **Gelöschte Objekte** aus (standardmäßig ist **Gelöschte Objekte** ein Unterordner von **Erweitert**).
2. Wählen Sie im Arbeitsbereich **Gelöschte Objekte** das gewünschte Objekt aus.

   Das Feld für die Arbeit mit dem ausgewählten Objekt wird auf der rechten Seite des Arbeitsbereichs angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Kasten auf den Link **Eigenschaften**.
   - Klicken Sie mit der rechten Maustaste auf das Objekt, das Sie im Arbeitsbereich ausgewählt haben und wählen Sie im Kontextmenü **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster des Objekts geöffnet, in dem folgende Registerkarten angezeigt werden:

   - **Allgemein**
   - **Revisionsverlauf**

Dauerhaftes Löschen von Objekten aus der Liste der gelöschten Objekte

Nur Benutzer mit der Berechtigung **Ändern** im Berechtigungsbereich **Gelöschte Objekte** können Objekte dauerhaft aus der Liste der gelöschten Objekte löschen (weitere Informationen finden Sie unter Zuweisen von Berechtigungen an Benutzer und Gruppen).

Um ein Objekt aus der Liste der gelöschten Objekte zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten des gewünschten Administrationsservers und wählen Sie dann den Ordner **Gelöschte Objekte** aus.
2. Wählen Sie im Arbeitsbereich die Objekte aus, die Sie löschen möchten.
3. Führen Sie eine der folgenden Aktionen aus:

   - Drücken Sie die Taste **Entf**.
   - Wählen Sie im Kontextmenü der ausgewählten Objekte die Option **Löschen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

   Das Objekt wird dauerhaft aus der Liste der gelöschten Objekte gelöscht. Alle Informationen über dieses Objekt (einschließlich aller Revisionen) werden dauerhaft aus der Datenbank entfernt. Diese Informationen können nicht wiederhergestellt werden.

Verwaltung mobiler Geräte

Die Verwaltung von mobilen Geräten über Kaspersky Security Center erfolgt mithilfe der Komponente "Verwaltung mobiler Geräte", die eine eigene Lizenz erfordert. Sie müssen die Komponente "Verwaltung mobiler Geräte" aktivieren, wenn Sie planen, die mobilen Geräte der Mitarbeiter Ihres Unternehmens zu verwalten.

Dieser Abschnitt enthält eine Anleitung zum Aktivieren, Deaktivieren und Anpassen der Komponente "Verwaltung mobiler Geräte". In diesem Abschnitt wird außerdem beschrieben, wie Sie Verwaltung mobiler Geräte können, die mit dem Administrationsserver verbunden sind.

Weitere Informationen zu Kaspersky Security für mobile Endgeräte entnehmen Sie bitte der *Hilfe zu Kaspersky Security für mobile Endgeräte*.

Szenario: Bereitstellung der Funktion "Verwaltung mobiler Geräte"

Dieser Abschnitt enthält ein Szenario zur Konfiguration der Funktionalität "Verwaltung mobiler Geräte" in Kaspersky Security Center.

Erforderliche Vorrausetzungen

Stellen Sie sicher, dass Sie eine Lizenz besitzen, welche die Funktionalität "Verwaltung mobiler Geräte" abdeckt.

Schritte

Die Bereitstellung der Funktionalität "Verwaltung mobiler Geräte" erfolgt in mehreren Schritten:

1. **Ports vorbereiten**

   Stellen Sie sicher, dass Port 13292 auf dem Administrationsserver verfügbar ist. Dieser Port wird für die Verbindung mit mobilen Geräten benötigt. In gewissen Fällen sollten Sie auch Port 17100 verfügbar machen. Dieser Port wird nur für den Proxyserver für die Aktivierung von verwalteten mobilen Geräten benötigt; wenn die verwalteten mobilen Geräte Internetzugang haben, muss dieser Port nicht verfügbar sein.

2. **Aktivieren der Funktion "Verwaltung mobiler Geräte"**

   Sie können die Funktionalität "Mobile Geräte verwalten" aktivieren, während der Schnellstartassistent für den Administrationsserver ausgeführt wird, oder zu einem späteren Zeitpunkt.

3. **Externe Adresse des Administrationsservers angeben**

   Sie können die externe Adresse während der Ausführung des Schnellstartassistenten für den Administrationsserver oder später angeben. Wenn sie die Funktion "Verwaltung mobiler Geräte" nicht bei der Installation ausgewählt und die Adresse nicht im Installationsassistenten angegeben haben, geben Sie die externe Adresse in den Eigenschaften des Installationspakets an.

4. **Mobile Geräte zur Gruppe "Verwaltete Geräte" hinzufügen**

   Fügen Sie die mobilen Geräte zur Gruppe "Verwaltete Geräte" hinzu, um sie mithilfe von Richtlinien zu verwalten. Sie können eine Regel für das Verschieben in einem der Schritte des Schnellstartassistenten für den Administrationsserver erstellen. Sie können eine Regel für das Verschieben auch später erstellen. Wenn Sie keine derartige Regel erstellen, können Sie mobile Geräte manuell zur Gruppe "Verwalteter Geräte" hinzufügen.

   Sie können mobile Geräte entweder direkt zur Gruppe "Verwalteter Geräte" hinzufügen, oder Sie erstellen eine Untergruppe (oder mehrere Untergruppen) für sie.

   Sie können später jederzeit neue mobile Geräte mithilfe des Assistenten für die Verbindung eines mobilen Gerätes mit dem Administrationsserver verbinden.

5. **Eine Richtlinie für mobile Geräte erstellen**

   Um mobile Geräte zu verwalten, erstellen Sie für diese eine Richtlinie (oder mehrere Richtlinien) in der Gruppe, welcher sie angehören. Sie können die Einstellungen dieser Richtlinie später jederzeit ändern.

Ergebnisse

Nach Abschluss dieses Szenarios können Sie Android- und iOS-Geräte mit Kaspersky Security Center verwalten. Das Arbeiten mit Zertifikaten von mobilen Geräten und Senden von Befehlen an mobile Geräte ist möglich.

Gruppenrichtlinie für die Verwaltung von iOS MDM-Geräten

Sie können zur Verwaltung von iOS MDM-Geräten das Verwaltungs-Plug-in von Kaspersky Device Management für iOS verwenden, das zum Lieferumfang von Kaspersky Security Center gehört. Kaspersky Device Management für iOS erlaubt Ihnen, Gruppenrichtlinien zum Anpassen von Konfigurationseinstellungen für iOS MDM-Geräte zu erstellen, ohne das iPhone® Configuration Utility verwenden zu müssen.

Eine Gruppenrichtlinie zum Verwalten von iOS MDM-Geräten bietet dem Administrator die folgenden Optionen:

- Sicherheitseinstellungen für die Verwendung des Kennworts auf dem Gerät anpassen.
- Beschränkungen für die Verwendung der Hardwarefunktionen des Geräts sowie Beschränkungen für die Installation und Deinstallation von mobilen Apps anpassen.
- Beschränkungen für die Verwendung der auf dem Gerät integrierten mobilen Apps, beispielsweise YouTube™, iTunes® Store, Safari, anpassen.
- Beschränkungen für die Anzeige von Medieninhalten (beispielsweise Filme und Fernsehsendungen) nach der Region anpassen, in der das Gerät benutzt wird.
- Internetverbindungseinstellungen des Geräts über einen Proxyserver (Globaler HTTP-Proxy) anpassen.
- Konfigurieren des Benutzerkontos, mit dem der Benutzer Zugang zu den Anwendungen und Diensten des Unternehmens erhält (Single Sign On-Technologie (SSO)).
- Internetnutzung (Besuch von Websites) auf den mobilen Geräten kontrollieren.
- Einstellungen von kabellosen Netzwerken (WLAN), Zugriffspunkten (APN), virtuellen privaten Netzwerken (VPN) mithilfe verschiedenster Authentifizierungsmechanismen und Netzwerkprotokollen anpassen.
- Verbindungseinstellungen von AirPlay®-Geräten zum Streamen von Fotos, Musik und Videos anpassen.
- Verbindungseinstellungen von AirPrint™-Druckern zum kabellosen Drucken von Dokumenten vom Gerät anpassen.
- Synchronisierungseinstellungen mit dem Microsoft Exchange Server sowie Benutzerkonten für die Nutzung der Unternehmens-E-Mail auf den Geräten anpassen.
- Anmeldedaten für die Synchronisierung mit dem Katalogdienst LDAP anpassen.
- Anmeldedaten für die Verbindung mit den Diensten CalDAV und CardDAV anpassen, wodurch der Benutzer Unternehmenskalender und Kontaktlisten verwenden kann.
- Einstellungen der iOS-Benutzeroberfläche auf dem Benutzergerät anpassen, beispielsweise Schriftarten oder Symbole für ausgewählte Websites.
- Neue Sicherheitszertifikate zum Gerät hinzufügen.

- Einstellungen des SCEP-Servers (Simple Certificate Enrollment-Protokoll) für den automatischen Erhalt von Zertifikaten von der Zertifizierungsstelle anpassen.

- Eigene Einstellungen für die Ausführung von mobilen Apps hinzufügen.

Die Besonderheit der Richtlinie zur Verwaltung von iOS MDM-Geräten liegt darin, dass sie einer Administrationsgruppe zugewiesen wird, zu welcher der iOS MDM-Server gehört (im Folgenden auch "Server für mobile Geräte"). Alle Einstellungen, die in dieser Richtlinie festgelegt sind, werden zunächst auf den Server für mobile Geräte und anschließend auf die von ihm verwalteten mobilen Geräte angewendet. Falls eine hierarchische Struktur von Administrationsgruppen verwendet wird, erhalten die sekundären Server für mobile Geräte die Einstellungen der Richtlinie von den primären Servern für mobile Geräte und verteilen sie an die mobilen Geräte.

Nähere Informationen zur Verwendung der Gruppenrichtlinie beim Verwalten von iOS MDM-Geräten in der Kaspersky Security Center Verwaltungskonsole, finden Sie in der Dokumentation zu *Kaspersky Security für mobile Endgeräte*.

Aktivieren der Funktion "Verwaltung mobiler Geräte"

Damit Sie mobile Geräte verwalten können, müssen Sie die Komponente "Verwaltung mobiler Geräte" aktivieren. Wenn Sie diese Komponente nicht im Schnellstartassistenten aktiviert haben, können Sie diese später aktivieren. Die Komponente "Verwaltung mobiler Geräte" erfordert eine Lizenz.

Die Komponente "Verwaltung mobiler Geräte" kann nur auf dem primären Administrationsserver aktiviert werden.

Um die Komponente "Verwaltung mobiler Geräte" zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte** aus.

2. Klicken Sie im Arbeitsbereich des Ordners auf die Schaltfläche **Verwaltung mobiler Geräte aktivieren**. Diese Schaltfläche ist nur verfügbar, wenn Sie **Verwaltung mobiler Geräte** nicht schon zuvor aktiviert haben.

   Die Seite **Zusätzliche Komponenten** des Schnellstartassistenten für den Administrationsserver wird angezeigt.

3. Wählen Sie **Verwaltung mobiler Geräte aktivieren**, um mobile Geräte zu verwalten.

4. Aktivieren Sie mittels Schlüsseldatei oder Aktivierungscode die Anwendung auf der Seite **Methode für die Programmaktivierung auswählen**.

   Die Verwaltung mobiler Geräte ist ohne Aktivierung der Funktionalität "Verwaltung mobiler Geräte" nicht verfügbar.

5. Aktivieren Sie auf der Seite **Proxyserver-Einstellungen für Internetzugriff** das Kontrollkästchen **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn dieses Kontrollkästchen aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die Verbindungseinstellungen für den Proxyserver.

6. Wählen Sie auf der Seite **Updates für Plug-ins und Installationspakete prüfen** eine der folgenden Optionen aus:

   - **Prüfen, ob Plug-ins und Installationspakete aktuell sind**

     Start der Untersuchung auf Aktualität. Wenn die Untersuchung veraltete Versionen der Plug-ins oder Installationspakete findet, bietet der Assistent an, anstelle der veralteten Versionen die aktuellen herunterzuladen.

- **Untersuchung überspringen**

  Fortsetzung der Ausführung ohne Untersuchung der Plug-ins und Installationspakete auf Aktualität. Diese Variante kann beispielsweise ausgewählt werden, wenn Sie keinen Zugriff auf das Internet haben oder aus einem bestimmten Grund die veraltete Programmversion weiter benutzen möchten.

  Das Überspringen der Untersuchung der Aktualität von Plug-ins kann zur inkorrekten Ausführung des Programms führen.

7. Laden Sie die neuesten Versionen der Plug-ins auf der Seite **Verfügbare neueste Plug-in-Versionen** in der gewünschten Sprache herunter und installieren Sie diese. Für das Update der Plug-ins ist keine Lizenz erforderlich.

   Nach der Installation der Plug-ins und der Pakete prüft das Programm, ob alle für die korrekte Funktion der mobilen Geräte notwendigen Plug-ins installiert wurden. Wenn veraltete Versionen der Plug-ins gefunden werden, fordert der Assistent Sie auf, die aktuellen Versionen herunterzuladen und die veralteten zu ersetzen.

8. Stellen Sie die Ports des Administrationsservers auf der Seite **Verbindungseinstellungen für mobile Geräte** ein.

Nach Fertigstellen des Assistenten werden die folgenden Änderungen vorgenommen:

- eine Richtlinie von Kaspersky Endpoint Security für Android wird erstellt
- eine Richtlinie von Kaspersky Device Management für iOS wird erstellt
- auf dem Administrationsserver werden Verbindungsports für mobile Geräte geöffnet

Einstellungen der Komponente "Verwaltung mobiler Geräte" anpassen

Um die Unterstützung für mobile Geräte zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte** aus.
2. Klicken Sie im Arbeitsbereich des Ordners auf den Link **Verbindungsports für mobile Geräte**.

   Der Abschnitt **Zusätzliche Ports** des Eigenschaftenfensters des Administrationsservers wird angezeigt.
3. Ändern Sie im Abschnitt **Zusätzliche Ports** die gewünschten Einstellungen:

   - **SSL-Port des Aktivierungs-Proxyservers**
   - **Port für mobile Geräte öffnen**

     Es wird ein Port für mobile Geräte zur Verbindung mit dem Lizenzserver geöffnet. Sie können die Portnummer und andere Einstellungen in den Feldern weiter unten festlegen.

     Diese Option ist standardmäßig aktiviert.
   - **Port zur Synchronisierung mobiler Geräte**

     Portnummer, über den die mobilen Geräte mit dem Administrationsserver verbunden werden und Informationen mit ihm austauschen. Standardmäßig wird Portnummer 13292 verwendet.

     Sie können einen anderen Port angeben, wenn Port 13292 für andere Zwecke verwendet wird.

- **Port zur Aktivierung mobiler Geräte**

  Port für die Verbindung von Kaspersky Endpoint Security für Android mit den Aktivierungsservern von Kaspersky.

  Standardmäßig wird Portnummer 17100 verwendet.

4. Klicken Sie auf die Schaltfläche **OK**.

Komponente "Verwaltung mobiler Geräte" deaktivieren

Die Komponente "Verwaltung mobiler Geräte" kann nur auf dem primären Administrationsserver deaktiviert werden.

Um die Komponente "Verwaltung mobiler Geräte" zu deaktivieren:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte** aus.
2. Klicken Sie im Arbeitsbereich des Ordners auf den Link **Zusätzliche Komponenten konfigurieren**.

   Die Seite **Zusätzliche Komponenten** des Schnellstartassistenten für den Administrationsserver wird angezeigt.
3. Wenn Sie keine mobilen Geräte mehr verwalten möchten, wählen Sie **Verwaltung mobiler Geräte deaktivieren** aus.
4. Klicken Sie auf die Schaltfläche **OK**.

Früher verbundene mobile Geräte können keine Verbindung zum Administrationsserver herstellen. Der Port zum Verbinden der mobilen Geräte und der Port zur Aktivierung von mobilen Geräten werden automatisch geschlossen.

Die erstellten Richtlinien von Kaspersky Endpoint Security für Android und Kaspersky Device Management für iOS werden nicht gelöscht. Die Regeln für das Ausstellen von Zertifikaten werden nicht verändert. Die installierten Plug-ins werden nicht entfernt. Die Verschiebungsregel für mobile Geräte wird nicht gelöscht.

Nach einer wiederholten Aktivierung von "Verwaltung mobiler Geräte" kann eine Neuinstallation der für die Verwaltung der mobilen Geräte erforderlichen mobilen Anwendungen auf den verwalteten mobilen Geräten erforderlich sein.

Arbeiten mit Befehlen für mobile Geräte

Dieser Abschnitt enthält Informationen über die Befehle für die Verwaltung von mobilen Geräten, die von Kaspersky Security Center unterstützt werden. Es werden Anleitungen für das Versenden der Befehle an die mobilen Geräte sowie für die Anzeige des Ausführungsstatus der Befehle im Befehlsprotokoll angeführt.

Befehle zur Verwaltung mobiler Geräte

Kaspersky Security Center unterstützt Befehle Verwaltung mobiler Geräte.

Die Befehle werden zur Remote-Verwaltung mobiler Geräte verwendet. Im Fall des Verlusts eines mobilen Geräts können mithilfe von Befehlen beispielsweise Unternehmensdaten vom Gerät gelöscht werden.

Sie können für folgende Typen von verwalteten mobilen Geräten Befehle verwenden:

- iOS MDM-Geräte
- KES-Geräte

Jeder Gerätetyp unterstützt eine bestimmte Auswahl von Befehlen.

Besonderheiten einiger Befehle

- Für alle Gerätetypen werden bei erfolgreicher Ausführung des Befehls **Auf Werkseinstellungen zurücksetzen** alle Daten vom Gerät gelöscht und die Geräteeinstellungen auf die Werkseinstellung zurückgesetzt.
- Für das iOS MDM-Gerät werden bei erfolgreicher Ausführung des Befehls **Unternehmensdaten löschen** alle voreingestellten Konfigurationsprofile, Provisioning-Profile, das iOS MDM-Profil und die Apps, für die das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren** aktiviert wurde, gelöscht.
- Für das KES-Gerät werden bei erfolgreicher Ausführung des Befehls **Unternehmensdaten löschen** die Unternehmensdaten, Einträge in Kontakten, der SMS-Verlauf, die Anrufliste, der Kalender, die Einstellungen für die Internetverbindung, die Benutzerkonten mit Ausnahme des Google™-Benutzerkontos vom Gerät gelöscht. Außerdem werden für das KES-Gerät die Daten von der Speicherkarte gelöscht.
- Vor dem Senden des Befehls **Gerät orten** an das KES-Gerät, müssen Sie bestätigen, dass Sie diesen Befehl für die sanktionierte Suche eines verlorenen Geräts verwenden, das Ihrem Unternehmen oder einem der Mitarbeiter gehört. Ein mobiles Gerät, das den Befehl **Gerät orten** empfängt ist nicht gesperrt.

Die Liste der Befehle der mobilen Geräte

In der Tabelle unten ist die Liste der Befehle für iOS MDM-Geräte angeführt.

Unterstützte Befehle zur Verwaltung mobiler Geräte: iOS MDM-Geräte

Befehle	Ergebnis der Befehlsausführung
Sperren	Das mobile Gerät wurde gesperrt.
Entsperren	Blockierung des mobilen Geräts mit PIN-Code ist deaktiviert. Der früher festgelegte PIN-Code wurde zurückgesetzt.
Auf Werkseinstellungen zurücksetzen	Sämtliche Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf die Werkseinstellung zurückgesetzt
Unternehmensdaten löschen	Alle installierten Konfigurationsprofile, Provisioning-Profile, iOS MDM-Profile und Apps, für die das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren** aktiviert ist, wurden gelöscht.
Gerät synchronisieren	Die Daten auf dem mobilen Gerät wurden mit dem Administrationsserver synchronisiert.
Profil installieren	Auf dem mobilen Gerät wurde ein Konfigurationsprofil installiert.
Profil entfernen	Das Konfigurationsprofil wurde vom mobilen Gerät gelöscht.

Befehle	Ergebnis der Befehlsausführung
Provisioning-Profil installieren	Auf dem mobilen Gerät wurde ein Provisioning-Profil installiert.
Provisioning-Profil entfernen	Das Provisioning-Profil wurde vom mobilen Gerät gelöscht.
App installieren	Auf dem mobilen Gerät wurde eine App installiert.
App löschen	Die App wurde vom mobilen Gerät gelöscht.
Gutschein-Code eingeben	Ein Gutscheincode für eine kostenpflichtige App wurde eingegeben.
Roaming konfigurieren	Daten-Roaming und Sprach-Roaming wurden aktiviert bzw. deaktiviert.

In der Tabelle unten ist die Liste der Befehle für KES-Geräte angeführt.

Unterstützte Befehle zur Verwaltung mobiler Geräte: KES-Geräte

Befehl	Ergebnis der Befehlsausführung
Sperren	Das mobile Gerät wurde gesperrt.
Entsperren	Blockierung des mobilen Geräts mit PIN-Code ist deaktiviert. Der früher festgelegte PIN-Code wurde zurückgesetzt.
Auf Werkseinstellungen zurücksetzen	Sämtliche Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf die Werkseinstellung zurückgesetzt
Unternehmensdaten löschen	Unternehmensdaten, Einträge in den Kontakten, SMS-Verlauf, Anrufliste, Kalender, Internetverbindungseinstellungen, Benutzerkonten außer dem Google-Benutzerkonto wurden gelöscht. Daten auf Speicherkarten wurden gelöscht.
Gerät synchronisieren	Die Daten auf dem mobilen Gerät wurden mit dem Administrationsserver synchronisiert.
Gerät orten	Der Standort des mobilen Geräts wurde ermittelt und auf Google Maps™ angezeigt. Der Mobilfunkanbieter erhebt Gebühren für den SMS-Versand und die Verbindung mit dem Internet.
Geheimes Foto	Das mobile Gerät wurde gesperrt. Mit der Frontkamera des Geräts wurde ein Foto aufgenommen und auf dem Administrationsserver gespeichert. Die Fotos können im Befehlsprotokoll angezeigt werden. Der Mobilfunkanbieter erhebt Gebühren für den SMS-Versand und die Verbindung mit dem Internet.
Alarmsignal erzeugen	Das mobile Gerät erzeugt ein Alarmsignal.

Verwendung von Firebase Cloud Messaging

Zur rechtzeitigen Zustellung von Befehlen auf KES-Geräten die durch das Android-Betriebssystem verwaltet werden, wird in Kaspersky Security Center das System der Push-Benachrichtigung verwendet. Push-Benachrichtigungen zwischen KES-Geräten und dem Administrationsserver werden mittels Firebase Cloud Messaging (im Folgenden als FCM bezeichnet) ausgetauscht. In der Kaspersky Security Center Verwaltungskonsole können Sie die Einstellungen für Firebase Cloud Messaging festlegen, um KES-Geräte an den Dienst anzuschließen.

Um die Einstellungen für Firebase Cloud Messaging zu erhalten, müssen Sie über ein Google-Benutzerkonto verfügen.

So aktivieren die Verwendung von FCM:

1. Wählen Sie in der Verwaltungskonsole zuerst den Knoten **Verwaltung mobiler Geräte** aus und dann den Ordner **Mobile Geräte**.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Mobile Geräte**, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie im Ordnereinstellungen den Abschnitt **Einstellungen von Firebase Cloud Messaging**.

4. Geben Sie im Feld **Firebase-Projektnummer** die ID des FCM Sender ein.

5. Wählen Sie im Feld **Datei mit privatem Schlüssel (JSON-Format)** die Datei mit dem privaten Schlüssel aus.

   Bei der nächsten Synchronisierung mit dem Administrationsserver werden KES-Geräte, die durch das Android-Betriebssystem verwaltet werden, an den Dienst Firebase Cloud Messaging angeschlossen.

Sie können die Einstellungen für Firebase Cloud Messaging mithilfe der Schaltfläche **Einstellungen zurücksetzen** ändern.

Befehle absenden

Gehen Sie wie folgt vor, um einen Befehl an ein mobiles Gerät des Benutzers zu senden:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Wählen Sie das mobile Gerät des Benutzers, an das der Befehl gesendet werden soll.

3. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

4. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt mit dem Namen des Befehls, der an das mobile Gerät gesendet werden soll, und klicken Sie auf die Schaltfläche **Befehl senden**.

   Nachdem Sie auf die Schaltfläche **Befehl senden** geklickt haben, öffnet sich abhängig vom ausgewählten Befehl möglicherweise das Fenster zum Anpassen der erweiterten Einstellungen des Befehls. Wenn zum Beispiel der Befehl zum Löschen des Provisioning-Profils gesendet wird, müssen Sie das Provisioning-Profil auswählen, das vom mobilen Gerät gelöscht werden soll. Geben Sie im Fenster die erweiterten Einstellungen des Befehls ein und bestätigen Sie Ihre Auswahl. Daraufhin wird der Befehl an das mobile Gerät gesendet.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

5. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung mobiler Geräte** zu schließen.

Status von Befehlen im Befehlsprotokoll anzeigen

Im Befehlsprotokoll werden Informationen über alle Befehle gespeichert, die an mobile Geräte gesendet wurden. Das Befehlsprotokoll enthält Informationen über Uhrzeit und Datum der Absendung des Befehls an das mobile Gerät, Status der Befehle sowie eine detaillierte Beschreibung der Ergebnisse der Befehlsausführung. Beispielsweise wird im Fall der fehlerhaften Ausführung des Befehls im Befehlsprotokoll die Fehlerursache angezeigt. Die Einträge im Befehlsprotokoll werden nach 30 Tagen gelöscht.

Die an ein mobiles Gerät gesendeten Befehle können folgende Status aufweisen:

- *Wird ausgeführt* – der Befehl wurde an das mobile Gerät gesendet.

- *Abgeschlossen* – der Befehl wurde erfolgreich ausgeführt.

- *Beendet mit Fehler* – der Befehl konnte nicht ausgeführt werden.
- *Wird gelöscht* – der Befehl wird aus der an das mobile Gerät gesendeten Befehlswarteschlange gelöscht.
- *Gelöscht* – der Befehl wurde erfolgreich aus der an das mobile Gerät gesendeten Befehlswarteschlange gelöscht.
- *Löschen fehlgeschlagen* – der Befehl konnte nicht aus der an das mobile Gerät gesendeten Befehlswarteschlange gelöscht werden.

Das Programm führt für jedes mobile Gerät ein Befehlsprotokoll.

Gehen Sie wie folgt vor, um das Befehlsprotokoll für an ein mobiles Gerät gesendete Befehle anzuzeigen:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Wählen Sie das mobile Gerät, für das Sie das Befehlsprotokoll anzeigen möchten, aus der Liste.

3. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

   Das Fenster **Befehle zur Verwaltung mobiler Geräte** wird geöffnet. Die Abschnitte im Fenster **Befehle zur Verwaltung mobiler Geräte** entsprechen den Befehlen, die an ein mobiles Gerät gesendet werden können.

4. Wählen Sie die Abschnitte mit den gewünschten Befehlen und lesen Sie im Block **Befehlsprotokoll** die Informationen über deren Ausführung.

Im Block **Befehlsprotokoll** werden eine Liste der an das mobile Gerät gesendeten Befehle sowie Informationen zu den Befehlen angezeigt. Mithilfe des Filters **Befehle zeigen** können Sie in der Liste nur Befehle mit dem ausgewählten Status anzeigen.

Zertifikate für mobile Geräte verwenden

Dieser Abschnitt enthält Informationen über die Arbeit mit Zertifikaten für mobile Geräte.

Das Root-Zertifikat für mobile Geräte hat nach seiner Generierung eine feste Ablauffrist von 700 Tagen. Das Reservezertifikat wird 60 Tage vor dem Ablaufdatum generiert. Sie können den Zeitraum für die Erstellung eines Reservezertifikats mit dem folgenden Befehl ändern:

```
klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <Timeout in Sekunden>
```

Der Zeitraum für die Erstellung eines Reservezertifikats muss lang genug sein, damit sich alle verwalteten mobilen Geräte mit dem Administrationsserver synchronisieren und das Zertifikat abrufen können.

Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

Die manuelle Verlängerung des Stammzertifikats für mobile Geräte wird nicht unterstützt.

Starten des Assistenten für die Installation eines Zertifikats

Auf den mobilen Geräten des Benutzers können die folgenden Typen von Zertifikaten installiert werden:

- Allgemeine Zertifikate zur Identifizierung des mobilen Geräts
- E-Mail-Zertifikate für die Konfiguration der Unternehmens-E-Mail auf dem mobilen Gerät
- VPN-Zertifikat für die Konfiguration des Zugriffs auf ein virtuelles privates Netzwerk auf dem mobilen Gerät

Gehen Sie wie folgt vor, um ein Zertifikat auf einem mobilen Gerät des Benutzers zu installieren:

1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Zertifikate** aus.
2. Starten Sie im Arbeitsbereich des Ordners **Zertifikate** mithilfe des Links **Zertifikat hinzufügen** den Assistenten für die Installation eines Zertifikats.

   Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wurde ein Zertifikat erstellt, zur Liste der Zertifikate des Benutzers hinzugefügt, und außerdem eine Benachrichtigung mit einem Link für den Download und die Installation des Zertifikats auf dem mobilen Gerät an den Benutzer gesendet. Sie können die Liste aller Zertifikate anzeigen und in eine Datei exportieren. Zertifikate können gelöscht und erneut ausgestellt werden. Darüber hinaus können Sie auch die Eigenschaften eines Zertifikats anzeigen.

Schritt 1. Auswählen des Zertifikattyps

Geben Sie den Typ des Zertifikats an, das auf dem mobilen Gerät des Benutzers installiert werden soll:

- **Mobiles Zertifikat** – zur Identifizierung des mobilen Gerätes
- **E-Mail-Zertifikat** – zur Konfiguration der Unternehmens-E-Mail auf dem mobilen Gerät
- **VPN-Zertifikat** – Konfiguration des Zugriffs auf ein virtuelles privates Netzwerk auf dem mobilen Gerät

Schritt 2. Auswählen des Gerätetyps

Dieses Fenster wird angezeigt, wenn als Zertifikatstyp **E-Mail-Zertifikat** oder **VPN-Zertifikat** ausgewählt wurde.

Geben Sie den Betriebssystem-Typ des Zielgeräts an:

- **iOS MDM-Gerät**. Wählen Sie diese Option aus, wenn das Zertifikat auf einem mobilen Gerät installiert werden soll, das über das iOS MDM-Protokoll mit dem iOS MDM-Server verbunden wird.

- **KES-Gerät, das von Kaspersky Security für mobile Geräte verwaltet wird**. Wählen Sie diese Option, wenn das Zertifikat auf einem KES-Gerät installiert werden soll. In diesem Fall wird das Zertifikat für die Identifizierung des Benutzers bei der Verbindung mit dem Administrationsserver verwendet.

- **KES-Gerät, das mit dem Administrationsserver ohne Authentifizierung über ein Benutzerzertifikat verbunden wird**. Wählen Sie diese Option, wenn das Zertifikat auf einem KES-Gerät ohne Authentifizierung über ein Zertifikat installiert werden soll. In diesem Fall muss der Administrator im letzten Schritt des Assistenten im Fenster **Benachrichtigungsmethode** den Typ der Autorisierung des Benutzers bei der Verbindung mit dem Administrationsserver auswählen.

Schritt 3. Auswählen eines Benutzers

Wählen Sie in der Liste die Benutzer, Sicherheitsgruppen oder Active Directory-Sicherheitsgruppen aus, für die Sie das Zertifikat installieren möchten.

Im Fenster **Benutzer auswählen** können Sie nach internen Benutzern von Kaspersky Security Center suchen. Sie können auf **Hinzufügen** klicken, um einen internen Benutzer hinzuzufügen.

Schritt 4. Auswählen der Zertifikatquelle

In diesem Fenster kann die Quelle des Zertifikats, mit dessen Hilfe der Administrationsserver das mobile Gerät identifiziert, ausgewählt werden. Sie können das Zertifikat auf eine der folgenden Arten angeben:

- Automatisch ein Zertifikat mithilfe des Administrationsservers erstellen und das Zertifikat auf dem Gerät hinzufügen.

- Die Datei eines früher erstellten Zertifikats angeben. Diese Methode ist nicht verfügbar, wenn im vorherigen Schritt mehrere Benutzer ausgewählt wurden.

Aktivieren Sie das Kontrollkästchen **Zertifikat veröffentlichen**, wenn die Benachrichtigung des Benutzers über das Erstellen des Zertifikates für sein mobiles Gerät erforderlich ist.

Wenn das mobile Gerät des Benutzers bereits früher gemäß dem Zertifikat autorisiert war und es keine Notwendigkeit gibt, den Benutzerkonto-Namen und das Kennwort anzugeben, um ein neues Zertifikat zu erhalten, deaktivieren Sie das Kontrollkästchen **Zertifikat veröffentlichen**. In diesem Fall wird das Fenster **Benachrichtigungsmethode** nicht angezeigt.

Schritt 5. Zuweisen eines Tags zum Zertifikat

Das Fenster **Tag des Zertifikats** wird angezeigt. wenn **iOS MDM-Gerät** als **Gerätetyp** ausgewählt wurde.

In der Dropdown-Liste können Sie dem Zertifikat des iOS MDM-Geräts des Benutzers ein Tag zuweisen. Das Zertifikat mit dem zugewiesenen Tag kann spezielle Einstellungen haben, die für dieses Tag in den Eigenschaften der Richtlinie für Kaspersky Device Management für iOS festgelegt sind.

In der Dropdown-Liste werden Sie aufgefordert, das Tag *Zertifikatsvorlage 1*, *Zertifikatsvorlage 2* oder *Zertifikatsvorlage 3* auszuwählen. Sie können die Tags in den folgenden Abschnitten anpassen:

- Wenn im Fenster **Zertifikatstyp** der Typ **E-Mail-Zertifikat** ausgewählt war, werden die Einstellungen der Tags dafür in den Eigenschaften des Benutzerkontos Exchange ActiveSync der mobilen Geräte angepasst (**Verwaltete Geräte** → **Richtlinien** → Eigenschaften der Richtlinie für Kaspersky Device Management für iOS → Abschnitt **Exchange ActiveSync** → **Hinzufügen** → **Erweitert**).

- Wenn im Fenster **Zertifikatstyp** der Typ **VPN-Zertifikat** ausgewählt war, werden die Einstellungen der Tags dafür in den Eigenschaften des VPN-Netzwerks der mobilen Geräte angepasst (**Verwaltete Geräte** > **Richtlinien** > Eigenschaften der Richtlinie für Kaspersky Device Management für iOS > Abschnitt **VPN** > **Hinzufügen** > **Erweitert**). Die Einstellungen der Tags, die für VPN-Zertifikate verwendet werden, sind nicht verfügbar, wenn für das VPN-Netzwerk der Verbindungstyp L2TP, PPTP, oder IPSec (Cisco™) ausgewählt ist.

Schritt 6. Angeben der Veröffentlichungseinstellungen des Zertifikats

In diesem Fenster können Sie die folgenden Einstellungen für Zertifikatsausgabe festlegen:

- **Den Benutzer nicht über ein neues Zertifikat benachrichtigen**

  Aktivieren Sie diese Option, wenn Sie einem Benutzer keine Benachrichtigung über die Erstellung eines Zertifikats für das mobile Gerät des Benutzers senden möchten. In diesem Fall wird das Fenster **Benachrichtigungsmethode** nicht angezeigt.

  > Diese Option gilt nur für Geräte mit installiertem Kaspersky Endpoint Security für Android.

  Sie können diese Option beispielsweise aktivieren, wenn das mobile Gerät des Benutzers bereits zuvor mithilfe eines Zertifikats authentifiziert wurde und es daher nicht notwendig ist, einen Benutzerkonto-Namen und ein Kennwort für den Empfang eines neuen Zertifikats anzugeben.

- **Dem Gerät mehrfaches Quittieren eines einzelnen Zertifikats erlauben (Nur für Geräte, auf denen Kaspersky Endpoint Security für Android installiert ist)**

  Aktivieren Sie diese Option, wenn Kaspersky Security Center das Zertifikat jedes Mal, wenn es in Kürze abläuft oder auf dem Zielgerät nicht gefunden wird, automatisch erneut senden soll.

  Das Zertifikat wird einige Tage vor dem Ablaufdatum des Zertifikats automatisch erneut gesendet. Sie können die Anzahl an Tagen im Fenster Regeln für das Ausstellen von Zertifikaten festlegen.

  In manchen Fällen wird das Zertifikat nicht auf dem Gerät gefunden. Dies kann beispielsweise vorkommen, wenn der Benutzer Sicherheitsanwendung von Kaspersky auf dem Gerät neu installiert oder die Geräteeinstellungen und Daten auf Werkseinstellungen zurücksetzt. In diesem Fall überprüft Kaspersky Security Center die Geräte-ID beim nächsten Versuch des Geräts, eine Verbindung mit dem Administrationsserver herzustellen. Wenn das Gerät dieselbe ID wie bei der Ausgabe des Zertifikats hat, sendet die Anwendung das Zertifikat erneut an das Gerät.

Schritt 7. Auswählen der Methode zur Benachrichtigung von Benutzers

> Das Fenster wird nicht angezeigt bei gewähltem Gerätetyp **iOS MDM-Gerät** oder bei gewählter Option **Den Benutzer nicht über ein neues Zertifikat benachrichtigen**.

Im Fenster **Benachrichtigungsmethode** können Sie die Benachrichtigungseinstellungen anpassen, um den Benutzer über die Installation des Zertifikats auf dem mobilen Gerät zu benachrichtigen.

Geben Sie im Feld **Authentifizierungsmethode** den Autorisierungstyp des Benutzers an:

- **Anmeldedaten (Domäne oder Anmeldename)**

  In diesem Fall benutzt der Benutzer das Domänenkennwort oder Kennwort des Anmeldenamens von Kaspersky Security Center, um das neue Zertifikat zu erhalten.

- **Einmalkennwort**

  In diesem Fall erhält der Benutzer ein Einmalkennwort, das per E-Mail oder mithilfe von SMS versendet wird. Dieses Kennwort muss für den Erhalt des neuen Zertifikats angegeben werden.

  Diese Option ändert sich auf **Kennwort**, wenn Sie die Option **Dem Gerät den mehrfachen Empfang eines einzelnen Zertifikats erlauben (nur für Geräte, auf denen Sicherheitsanwendungen von Kaspersky für mobile Geräte installiert sind)** im Fenster **Einstellungen für Zertifikatsausgabe** aktiviert (ausgewählt) haben.

- **Kennwort**

  In diesem Fall wird das Kennwort jedes Mal verwendet, wenn das Zertifikat an den Benutzer gesendet wird.

  Diese Option ändert sich auf **Einmalkennwort**, wenn Sie die Option **Dem Gerät den mehrfachen Empfang eines einzelnen Zertifikats erlauben (nur für Geräte, auf denen Sicherheitsanwendungen von Kaspersky für mobile Geräte installiert sind)** im Fenster **Einstellungen für Zertifikatsausgabe** deaktiviert (entfernt) haben.

Das Feld wird angezeigt, wenn Sie **Mobiles Zertifikat** im Fenster **Zertifikatstyp** ausgewählt haben oder wenn Sie als Gerätetyp **KES-Gerät, das mit dem Administrationsserver ohne Authentifizierung über ein Benutzerzertifikat verbunden wird** ausgewählt haben.

Wählen Sie die Option zur Benachrichtigung des Benutzers aus:

- **Kennwort für die Authentifizierung nach Fertigstellen des Assistenten anzeigen**

  Wenn Sie diese Option auswählen, werden der Benutzername, der Benutzername in Security Account Manager (SAM) und das Kennwort für den Abruf des Zertifikats für jeden der ausgewählten Benutzer im abschließenden Schritt des Assistenten für die Installation eines Zertifikats angezeigt. Das Anpassen der Einstellungen für die Benachrichtigung des Benutzers über das installierte Zertifikat ist nicht verfügbar.

  Wenn Sie Zertifikate für mehrere Benutzer hinzufügen, können Sie die bereitgestellten Anmeldedaten in einer Datei speichern, indem Sie im letzten Schritt des Assistenten für die Installation eines Zertifikats auf die Schaltfläche **Exportieren** klicken.

  > Diese Option ist nicht verfügbar, wenn Sie **Anmeldedaten (Domäne oder Anmeldename)** im Schritt **Benachrichtigungsmethode** des Assistenten für die Installation eines Zertifikats ausgewählt haben.

- **Benutzer über das neue Zertifikat benachrichtigen**

  Bei der Auswahl dieser Variante können Sie die Einstellungen für die Benachrichtigung des Benutzers über ein neues Zertifikat anpassen.

  - **Per E-Mail**

    In dieser Einstellungsgruppe können Sie die Benachrichtigungseinstellungen anpassen, um den Benutzer per E-Mail-Nachricht über die Installation des Zertifikates auf seinem mobilen Gerät zu benachrichtigen. Diese Benachrichtigungsmethode ist nur verfügbar wenn der SMTP-Server angepasst wurde.

Klicken Sie auf den Link **Nachricht bearbeiten**, um den Benachrichtigungstext anzuzeigen und erforderlichenfalls zu ändern.

- **Mit SMS**

  In dieser Einstellungsgruppe können Sie die Benachrichtigung des Benutzers über die Verwendung von SMS zum Installieren eines Zertifikats auf mobilen Geräten anpassen. Diese Benachrichtigungsmethode ist nur verfügbar wenn die SMS-Nachrichten angepasst wurden.

  Klicken Sie auf den Link **Nachricht bearbeiten**, um den Benachrichtigungstext anzuzeigen und erforderlichenfalls zu ändern.

Schritt 8. Generieren des Zertifikats

Bei diesem Schritt wird das Zertifikat erstellt.

Klicken Sie auf **Fertigstellen** um den Assistenten abzuschließen.

Das generierte Zertifikat wird in der Liste der Zertifikate im Arbeitsbereich des Ordners **Zertifikate** erstellt und angezeigt.

Regeln für das Ausstellen von Zertifikaten anpassen

Die Zertifikate werden zur Authentifizierung des Geräts auf dem Administrationsserver verwendet. Alle verwalteten mobilen Geräte benötigen Zertifikate. Sie können festlegen, auf welche Weise die Zertifikate ausgestellt werden.

Um die Regeln für die Ausstellung eines Zertifikats anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Zertifikate** aus.

2. Öffnen Sie durch Klicken auf die Schaltfläche **Regeln für das Ausstellen von Zertifikaten anpassen** im Arbeitsbereich des Ordners **Zertifikate** das Fenster **Regeln für das Ausstellen von Zertifikaten**.

3. Gehen Sie zum Abschnitt mit dem Namen des Zertifikatstyps:

   Mobilgerät-Zertifikat ausstellen – für die Anpassung der Ausstellung von Zertifikaten auf mobilen Geräten.

   E-Mail-Zertifikate ausstellen – für die Anpassung der Ausstellung von E-Mail-Zertifikaten.

   Ausstellung von VPN-Zertifikaten – für die Anpassung der Ausstellung von VPN-Zertifikaten.

4. Passen Sie im Block **Ausstellungseinstellungen** die Ausstellung der Zertifikate wie folgt an:

   - Geben Sie die Gültigkeitsdauer des Zertifikats in Tagen an.

     Zertifikate für mobile Geräte sind durch das Ablaufdatum des Stammzertifikats eingeschränkt. Wenn Sie für das Zertifikats eine längere Laufzeit als das Ablaufdatum des Stammzertifikats angeben, wird die Laufzeit des Zertifikats bei der Erstellung automatisch angepasst.

   - Wählen Sie den Ursprung des Zertifikats (**Administrationsserver** oder **Zertifikate werden manuell erstellt**).

     Standardmäßig ist der Administrationsserver als Quelle für die Zertifikate ausgewählt.

- Geben Sie eine Zertifikatsvorlage an (**Standardvorlage**, **Andere Vorlage**).

  Die Anpassung von Vorlagen ist verfügbar, wenn im Abschnitt **PKI-Integration** die Funktion In Public-Key-Infrastruktur integrieren ausgewählt ist.

5. Passen Sie im Block **Einstellungen für das automatische Update** das automatische Update des Zertifikats an:

   - Geben Sie im Feld **Erneuerung bevor das Zertifikat abläuft in (Tagen)** an, wie viele Tage vor Ablauf der Gültigkeitsdauer das Zertifikat aktualisiert werden muss.
   - Aktivieren Sie das Kontrollkästchen **Zertifikat automatisch neu veröffentlichen, falls möglich**, um das automatische Aktualisieren der Zertifikate zu aktivieren.

6. Aktivieren Sie im Block **Kennwortschutz** die Verwendung eines Kennworts bei der Entschlüsselung von Zertifikate und passen Sie die Einstellungen an.

   Der Kennwortschutz ist nur für Mobilgerät-Zertifikate verfügbar.

   a. Aktivieren Sie das Kontrollkästchen **Bei der Installation des Zertifikats Kennwort abfragen**.

   b. Passen Sie mithilfe des Schiebereglers die maximale Anzahl von Zeichen im Kennwort für die Verschlüsselung an.

7. Klicken Sie auf die Schaltfläche **OK**.

Integration mit Public Key Infrastructure

Die Integration mit Public-Key-Infrastruktur (PKI) ist erforderlich, um die Ausstellung von Domänenzertifikaten der Benutzer zu vereinfachen. Die Integration der Zertifikatausstellung erfolgt daraufhin automatisch.

Die früheste unterstützte Version des PKI-Servers ist Windows Server 2008.

Das Benutzerkonto muss für die Integration mit PKI angepasst werden. Das Benutzerkonto muss folgenden Anforderungen genügen:

- Es muss Domänenbenutzer und Administrator des Geräts sein, auf dem der Administrationsserver installiert ist
- Es muss auf dem Gerät mit dem installierten Administrationsserver über die Berechtigung SeServiceLogonRight verfügen

Mit dem vorkonfigurierten Benutzerkonto muss auf dem Gerät, auf dem der Administrationsserver installiert ist, mindestens einmal eine Anmeldung durchgeführt werden, um ein ständiges Benutzerprofil zu erstellen. Im Zertifikatsspeicher dieses Benutzers auf dem Gerät mit dem Administrationsserver muss ein Zertifikat des Registrierungsagenten installiert werden, das von den Domänenadministratoren zur Verfügung gestellt wird.

Um die Integration mit Public-Key-Infrastruktur anzupassen, gehen Sie folgendermaßen vor:

1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Zertifikate** aus.

2. Klicken Sie im Arbeitsbereich auf **In Public-Key-Infrastruktur integrieren**, um den Abschnitt **PKI-Integration** des Fensters **Regeln für das Ausstellen von Zertifikaten** zu öffnen.

   Der Abschnitt **PKI-Integration** des Fensters **Regeln für das Ausstellen von Zertifikaten** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Zertifikatsausstellung in die PKI integrieren**.

4. Geben Sie im Feld **Benutzerkonto** den Benutzerkonto-Namen an, das für die Integration mit der Public-Key-Infrastruktur verwendet werden soll.

5. Geben Sie im Feld **Kennwort** das Domänenkennwort des Benutzerkontos an.

6. Wählen Sie in der Liste **Name der Zertifikatsvorlage im PKI-System** die Zertifikatsvorlage aus, auf deren Grundlage die Zertifikate für die Domänenbenutzer ausgestellt werden.

   Ein spezieller Dienst wird in Kaspersky Security Center unter dem angegebenen Benutzerkonto ausgeführt. Dieser Dienst ist für die Ausgabe der Domänenzertifikate des Benutzers verantwortlich. Der Dienst wird gestartet, wenn die Liste der Zertifikatsvorlagen mithilfe der Schaltfläche **Liste aktualisieren** heruntergeladen wird, oder wenn ein Zertifikat ausgestellt wird.

7. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

Die Integration der Zertifikatausstellung erfolgt daraufhin automatisch.

Unterstützung von Kerberos Constrained Delegation aktivieren

Das Programm unterstützt die Verwendung von Kerberos Constrained Delegation.

Um die Unterstützung von Kerberos Constrained Delegation zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte**.

2. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Server für mobile Geräte** aus.

3. Wählen Sie im Arbeitsbereich des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.

4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

5. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Einstellungen** aus.

6. Aktivieren Sie im Abschnitt **Settings** das Kontrollkästchen **Kompatibilität mit Kerberos Constrained Delegation gewährleisten**.

7. Klicken Sie auf die Schaltfläche **OK**.

Mobiles iOS-Gerät zur Liste der verwalteten Geräte hinzufügen

Um ein mobiles iOS-Gerät zur Liste der verwalteten Geräte hinzuzufügen, muss auf dem Gerät ein freigegebenes Zertifikat hinzugefügt und installiert werden. Freigegebene Zertifikate werden vom Administrationsserver verwendet, um mobile Geräte zu identifizieren. Ein freigegebenes Zertifikat für ein iOS-Mobilgerät wird innerhalb eines iOS MDM-Profils übermittelt. Nach der Zustellung und Installation eines freigegebenen Zertifikats auf dem mobilen Gerät wird das Gerät in der Liste der verwalteten Geräte angezeigt.

Kaspersky stellt die Unterstützung für Kaspersky Safe Browser ein.

Sie können mobile Benutzergeräte zur Liste der verwalteten Geräte hinzufügen. Dazu dient der "Assistent für die Verbindung eines mobilen Gerätes".

Um ein iOS-Gerät mithilfe eines freigegebenen Zertifikats mit dem Administrationsserver zu verbinden:

1. Starten Sie den "Assistenten für die Verbindung eines mobilen Gerätes" auf eine der folgenden Arten:

   - Verwenden Sie das Kontextmenü im Ordner **Benutzerkonten**:

     1. Erweitern Sie die Konsolenstruktur im Ordner **Erweitert** und wählen Sie den Unterordner **Benutzerkonten** aus.

     2. Wählen Sie im Arbeitsbereich des Ordners **Benutzerkonten** die Benutzer, die Sicherheitsgruppen oder die Active-Directory-Sicherheitsgruppen aus, deren mobile Geräte Sie zur Liste der verwalteten Geräte hinzufügen möchten.

     3. Führen Sie einen Rechtsklick aus und wählen Sie im Kontextmenü des Benutzerkontos die Option **Mobiles Gerät hinzufügen** aus.

        Der Assistent für die Verbindung eines mobilen Gerätes wird gestartet.

   - Klicken Sie im Arbeitsbereich des Ordners **Mobile Geräte** auf die Schaltfläche **Mobiles Gerät hinzufügen**:

     1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Mobile Geräte** aus.

     2. Klicken Sie im Arbeitsbereich des Unterordners **Mobile Geräte** auf die Schaltfläche **Mobiles Gerät hinzufügen**.

        Der Assistent für die Verbindung eines mobilen Gerätes wird gestartet.

2. Wählen Sie im Assistenten auf der Seite **Betriebssystem** als Typ des Mobilgerät-Betriebssystems **iOS** aus.

3. Wählen Sie "iOS MDM-Server" auf der Seite **iOS MDM-Server auswählen**.

4. Wählen Sie auf der Seite **Wählen Sie Benutzer aus, deren mobile Geräte Sie verwalten möchten** die Benutzer, Sicherheitsgruppen oder Active-Directory-Sicherheitsgruppen aus, deren mobile Geräte Sie zur Liste der verwalteten Geräte hinzufügen möchten.

   Dieser Schritt wird übersprungen, wenn Sie den Assistenten durch Auswahl von **Mobiles Gerät hinzufügen** im Kontextmenü des Ordners **Benutzerkonten** starten.

Falls Sie ein neues Benutzerkonto zur Liste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie im folgenden Fenster die Eigenschaften des Benutzerkontos ein. Falls Sie die Eigenschaften des Benutzerkontos ändern oder einsehen möchten, wählen Sie das Benutzerkonto in der Liste aus und klicken Sie auf **Eigenschaften**.

5. Geben Sie im Assistenten auf der Seite **Quelle des Zertifikats** an, wie das freigegebene Zertifikat erstellt werden soll, mit dem der Administrationsserver das mobile Gerät identifiziert. Sie können ein allgemeines Zertifikat auf eine von zwei Arten angeben:

   - **Zertifikat mittels Administrationsserver-Tools ausstellen**

     Wählen Sie diese Option aus, um mithilfe der Administrationsserver-Tools ein neues Zertifikat zu erstellen, falls Sie noch kein Zertifikat erstellt haben.

     Bei Auswahl dieser Option wird das iOS MDM-Profil automatisch anhand des Zertifikats signiert, das vom Administrationsserver erstellt wurde.

     Diese Variante ist standardmäßig festgelegt.

   - **Zertifikatdatei angeben**

     Wählen Sie diese Option aus, um ein Zertifikat anzugeben, das früher erstellt wurde.

     Diese Methode ist nicht verfügbar, wenn im vorherigen Schritt mehrere Benutzer ausgewählt wurden.

6. Passen Sie im Assistenten auf der Seite **Benachrichtigungsmethode** die Benachrichtigung an, mit welcher der Benutzer des mobilen Geräts per SMS-Nachricht oder E-Mail über die Erstellung eines Zertifikats informiert wird:

   - **QR-Code im Assistenten anzeigen**

     Bei der Auswahl dieser Variante wird im letzten Schritt des Assistenten für die Verbindung eines mobilen Gerätes der Link zum Installationspaket angezeigt.

     > Diese Variante ist nicht verfügbar, wenn mehrere Benutzer für die Verbindung des Geräts ausgewählt wurden.

   - **QR-Code an Benutzer senden**

     Bei der Auswahl dieser Variante können die Einstellungen für die Benachrichtigung des Benutzers über die Verbindung eines neuen mobilen Geräts angepasst werden.

     Sie können den Typ der E-Mail-Adresse auswählen, eine zusätzliche Adresse angeben und der Text der Nachricht bearbeiten. Sie können auch n kann auch den Typ des Nutzertelefons für den Versand der SMS-Nachricht auswählen, eine zusätzliche Rufnummer angeben und den Text der abgesandten SMS-Nachricht bearbeiten.

     Wenn der SMTP-Server nicht angepasst wurde, ist der Versand der E-Mail-Nachrichten an die Benutzer nicht möglich. Wenn die SMS-Benachrichtigungen nicht angepasst wurden, ist der Versand der SMS-Nachrichten an die Benutzer nicht möglich.

7. Klicken Sie auf der Seite **Ergebnis** auf **Fertigstellen**, um den Assistenten zu schließen.

Daraufhin wird das iOS MDM-Profil automatisch auf dem Kaspersky Security Center Webserver veröffentlicht. Der Benutzer des mobilen Geräts erhält eine Benachrichtigung mit dem Link zum Herunterladen des iOS MDM-Profils vom Webserver. Der Benutzer soll auf den empfangenen Link klicken. Daraufhin zeigt das Betriebssystem des mobilen Geräts dem Benutzer eine Zustimmungsaufforderung zur Installation des iOS MDM-Profils an. Damit das iOS MDM-Profil auf das mobile Gerät heruntergeladen wird, muss der Benutzer der Installation des iOS MDM-Profils zustimmen. Nach dem Herunterladen des iOS MDM-Profils und der Synchronisierung mit dem

Administrationsserver wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Verwaltung mobiler Geräte** der Konsolenstruktur angezeigt.

Damit der Benutzer über den erhaltenen Link auf den Kaspersky Security Center Webserver wechseln kann, ist es erforderlich, dass sein mobiles Gerät auf die Verbindung mit dem Administrationsserver über den Port 8061 zugreifen kann.

Mobiles Android-Gerät zur Liste der verwalteten Geräte hinzufügen

Um ein Android-Gerät zur Liste der verwalteten Geräte hinzuzufügen, müssen Kaspersky Endpoint Security für Android und ein freigegebenes Zertifikat an das mobile Gerät übermittelt und dort installiert werden. Freigegebene Zertifikate werden vom Administrationsserver verwendet, um mobile Geräte zu identifizieren. Nach der Zustellung und Installation eines freigegebenen Zertifikats auf dem mobilen Gerät wird das Gerät in der Liste der verwalteten Geräte angezeigt.

Sie können mobile Benutzergeräte zur Liste der verwalteten Geräte hinzufügen. Dazu dient der "Assistent für die Verbindung eines mobilen Gerätes". Der Assistent bietet zwei Optionen, um ein freigegebenes Zertifikat und Kaspersky Endpoint Security für Android zu übermitteln und zu installieren:

- Unter Verwendung eines Links für Google Play
- Unter Verwendung eines Links vom Kaspersky Security Center Webserver

  Das Installationspaket für Kaspersky Endpoint Security für Android, das zur Verteilung auf dem Administrationsserver gespeichert wurde, wird für die Installation verwendet

Assistent für die Verbindung eines mobilen Gerätes starten

Um den Assistenten für die Verbindung eines mobilen Gerätes zu starten, gehen Sie wie folgt vor:

- Verwenden Sie das Kontextmenü im Ordner **Benutzerkonten**:

  1. Erweitern Sie die Konsolenstruktur im Ordner **Erweitert** und wählen Sie den Unterordner **Benutzerkonten** aus.
  2. Wählen Sie im Arbeitsbereich des Ordners **Benutzerkonten** die Benutzer, die Sicherheitsgruppen oder die Active-Directory-Sicherheitsgruppen aus, deren mobile Geräte Sie zur Liste der verwalteten Geräte hinzufügen möchten.
  3. Führen Sie einen Rechtsklick aus und wählen Sie im Kontextmenü des Benutzerkontos die Option **Mobiles Gerät hinzufügen** aus.

     Der Assistent für die Verbindung eines mobilen Gerätes wird gestartet.

- Klicken Sie im Arbeitsbereich des Ordners **Mobile Geräte** auf die Schaltfläche **Mobiles Gerät hinzufügen**:

  1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Mobile Geräte** aus.
  2. Klicken Sie im Arbeitsbereich des Unterordners **Mobile Geräte** auf die Schaltfläche **Mobiles Gerät hinzufügen**.

     Der Assistent für die Verbindung eines mobilen Gerätes wird gestartet.

Hinzufügen eines Android-Gerätes mit einem Link für Google Play.

Um Kaspersky Endpoint Security für Android und ein freigegebenes Zertifikat mithilfe eines Links für Google Play auf einem mobilen Gerät zu installieren:

1. Starten Sie den Assistenten für die Verbindung eines mobilen Gerätes.
2. Wählen Sie im Assistenten auf der Seite **Betriebssystem** als Typ des Mobilgerät-Betriebssystems **Android** aus.
3. Auf der Seite **Methode zur Installation von Kaspersky Endpoint Security für Android auf Geräten** des Assistenten, wählen Sie die Option **Laden Sie die App von Google Play herunter**.
4. Wählen Sie auf der Seite **Wählen Sie Benutzer aus, deren mobile Geräte Sie verwalten möchten** des Assistenten die Benutzer, Sicherheitsgruppen oder Active-Directory-Sicherheitsgruppen aus, deren mobile Geräte Sie zur Liste der verwalteten Geräte hinzufügen möchten.

   Dieser Schritt wird übersprungen, wenn der Assistent durch Auswahl von **Mobiles Gerät hinzufügen** im Kontextmenü des Ordners **Benutzerkonten** gestartet wird.

   Falls Sie ein neues Benutzerkonto zur Liste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie im folgenden Fenster die Eigenschaften des Benutzerkontos ein. Falls Sie die Eigenschaften des Benutzerkontos ändern oder einsehen möchten, wählen Sie das Benutzerkonto in der Liste aus und klicken Sie auf **Eigenschaften**.
5. Geben Sie im Assistenten auf der Seite **Quelle des Zertifikats** an, wie das freigegebene Zertifikat erstellt werden soll, mit dem der Administrationsserver das mobile Gerät identifiziert. Sie können ein allgemeines Zertifikat auf eine von zwei Arten angeben:

   - **Zertifikat mittels Administrationsserver-Tools ausstellen**

     Wählen Sie diese Option aus, um mithilfe der Administrationsserver-Tools ein neues Zertifikat zu erstellen, falls Sie noch kein Zertifikat erstellt haben.

     Bei Auswahl dieser Option wird das Zertifikat automatisch durch den Administrationsserver ausgestellt.

     Diese Variante ist standardmäßig festgelegt.

   - **Zertifikatdatei angeben**

     Wählen Sie diese Option aus, um ein Zertifikat anzugeben, das früher erstellt wurde.

     Diese Methode ist nicht verfügbar, wenn im vorherigen Schritt mehrere Benutzer ausgewählt wurden.
6. Passen Sie im Assistenten auf der Seite **Benachrichtigungsmethode** die Benachrichtigung an, mit welcher der Benutzer des mobilen Geräts per SMS-Nachricht oder E-Mail über die Erstellung eines Zertifikats informiert wird:

   - **QR-Code im Assistenten anzeigen**

     Bei der Auswahl dieser Variante wird im letzten Schritt des Assistenten für die Verbindung eines mobilen Gerätes der Link zum Installationspaket angezeigt.

     Diese Variante ist nicht verfügbar, wenn mehrere Benutzer für die Verbindung des Geräts ausgewählt wurden.

- **QR-Code an Benutzer senden**

  Bei der Auswahl dieser Variante können die Einstellungen für die Benachrichtigung des Benutzers über die Verbindung eines neuen mobilen Geräts angepasst werden.

  Sie können den Typ der E-Mail-Adresse auswählen, eine zusätzliche Adresse angeben und der Text der Nachricht bearbeiten. Sie können auch n kann auch den Typ des Nutzertelefons für den Versand der SMS-Nachricht auswählen, eine zusätzliche Rufnummer angeben und den Text der abgesandten SMS-Nachricht bearbeiten.

  Wenn der SMTP-Server nicht angepasst wurde, ist der Versand der E-Mail-Nachrichten an die Benutzer nicht möglich. Wenn die SMS-Benachrichtigungen nicht angepasst wurden, ist der Versand der SMS-Nachrichten an die Benutzer nicht möglich.

7. Klicken Sie auf der Seite **Ergebnis** auf **Fertigstellen**, um den Assistenten zu schließen.

Daraufhin werden ein Link und ein QR-Code zum Herunterladen von Kaspersky Endpoint Security für Android an das mobile Gerät des Benutzers gesendet. Der Benutzer klickt auf den Link oder scannt den QR-Code. Daraufhin zeigt das Betriebssystem des mobilen Geräts dem Benutzer eine Zustimmungsaufforderung zur Installation von Kaspersky Endpoint Security für Android an. Nach dem Herunterladen und der Installation von Kaspersky Endpoint Security für Android stellt das mobile Gerät eine Verbindung zum Administrationsserver her und lädt das allgemeine Zertifikat herunter. Nach der Installation des Zertifikats auf dem mobilen Gerät wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Verwaltung mobiler Geräte** der Konsolenstruktur angezeigt.

Hinzufügen eines mobilen Gerätes mithilfe eines Links des Kaspersky Security Center Webservers

Für die Installation wird das Installationspaket für Kaspersky Endpoint Security für Android verwendet, das auf dem Administrationsserver veröffentlicht wurde.

Um Kaspersky Endpoint Security für Android und ein freigegebenes Zertifikat mithilfe eines Webserver-Links auf einem mobilen Gerät zu installieren:

1. Starten Sie den Assistenten für die Verbindung eines mobilen Gerätes.

2. Wählen Sie im Assistenten auf der Seite **Betriebssystem** als Typ des Mobilgerät-Betriebssystems **Android** aus.

3. Auf der Seite **Methode zur Installation von Kaspersky Endpoint Security für Android auf Geräten** des Assistenten, wählen Sie die Option **Laden Sie das Installationspaket der App von Kaspersky Security Center herunter**.

   Wählen Sie im folgenden Feld ein Installationspaket aus oder erstellen Sie ein neues Installationspaket über die Schaltfläche **Neu**.

4. Wählen Sie auf der Seite **Wählen Sie Benutzer aus, deren mobile Geräte Sie verwalten möchten** des Assistenten die Benutzer, Sicherheitsgruppen oder Active-Directory-Sicherheitsgruppen aus, deren mobile Geräte Sie zur Liste der verwalteten Geräte hinzufügen möchten.

   Dieser Schritt wird übersprungen, wenn der Assistent durch Auswahl von **Mobiles Gerät hinzufügen** im Kontextmenü des Ordners **Benutzerkonten** gestartet wird.

Falls Sie ein neues Benutzerkonto zur Liste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie im folgenden Fenster die Eigenschaften des Benutzerkontos ein. Falls Sie die Eigenschaften des Benutzerkontos ändern oder einsehen möchten, wählen Sie das Benutzerkonto in der Liste aus und klicken Sie auf **Eigenschaften**.

5. Geben Sie im Assistenten auf der Seite **Quelle des Zertifikats** an, wie das freigegebene Zertifikat erstellt werden soll, mit dem der Administrationsserver das mobile Gerät identifiziert. Sie können ein allgemeines Zertifikat auf eine von zwei Arten angeben:

   - **Zertifikat mittels Administrationsserver-Tools ausstellen**

     Wählen Sie diese Option aus, um mithilfe der Administrationsserver-Tools ein neues Zertifikat zu erstellen, falls Sie noch kein Zertifikat erstellt haben.

     Bei Auswahl dieser Option wird das Zertifikat automatisch durch den Administrationsserver ausgestellt.

     Diese Variante ist standardmäßig festgelegt.

   - **Zertifikatdatei angeben**

     Wählen Sie diese Option aus, um ein Zertifikat anzugeben, das früher erstellt wurde.

     Diese Methode ist nicht verfügbar, wenn im vorherigen Schritt mehrere Benutzer ausgewählt wurden.

6. Passen Sie im Assistenten auf der Seite **Benachrichtigungsmethode** die Benachrichtigung an, mit welcher der Benutzer des mobilen Geräts per SMS-Nachricht oder E-Mail über die Erstellung eines Zertifikats informiert wird:

   - **QR-Code im Assistenten anzeigen**

     Bei der Auswahl dieser Variante wird im letzten Schritt des Assistenten für die Verbindung eines mobilen Gerätes der Link zum Installationspaket angezeigt.

     > Diese Variante ist nicht verfügbar, wenn mehrere Benutzer für die Verbindung des Geräts ausgewählt wurden.

   - **QR-Code an Benutzer senden**

     Bei der Auswahl dieser Variante können die Einstellungen für die Benachrichtigung des Benutzers über die Verbindung eines neuen mobilen Geräts angepasst werden.

     Sie können den Typ der E-Mail-Adresse auswählen, eine zusätzliche Adresse angeben und der Text der Nachricht bearbeiten. Sie können auch n kann auch den Typ des Nutzertelefons für den Versand der SMS-Nachricht auswählen, eine zusätzliche Rufnummer angeben und den Text der abgesandten SMS-Nachricht bearbeiten.

     Wenn der SMTP-Server nicht angepasst wurde, ist der Versand der E-Mail-Nachrichten an die Benutzer nicht möglich. Wenn die SMS-Benachrichtigungen nicht angepasst wurden, ist der Versand der SMS-Nachrichten an die Benutzer nicht möglich.

7. Klicken Sie auf der Seite **Ergebnis** auf **Fertigstellen**, um den Assistenten zu schließen.

Daraufhin wird das Paket mit mobilen Apps für Kaspersky Endpoint Security für Android-Geräte automatisch auf dem Kaspersky Security Center Webserver veröffentlicht. Das Paket mit mobilen Apps enthält die App, die Verbindungseinstellungen des mobilen Geräts für den Administrationsserver und das Zertifikat. Der Benutzer des mobilen Geräts erhält eine Benachrichtigung mit dem Link zum Herunterladen des Pakets vom Webserver. Der Benutzer soll auf den empfangenen Link klicken. Danach fordert das Betriebssystem des Gerätes den Benutzer auf, die Installation des Pakets mit der mobilen App zu bestätigen. Stimmt der Benutzer zu, wird das Paket auf das mobile Gerät heruntergeladen. Nach dem Herunterladen des Pakets und der Synchronisierung mit dem

Administrationsserver wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Verwaltung mobiler Geräte** der Konsolenstruktur angezeigt.

iOS MDM-Geräte verwalten

In diesem Abschnitt werden die zusätzlichen Möglichkeiten zur Verwaltung von iOS MDM-Geräten mithilfe von Kaspersky Security Center beschrieben. Das Programm bietet folgende Möglichkeiten zur Verwaltung von iOS MDM-Geräten:

- Einstellungen für die verwalteten iOS MDM-Geräte zentral anpassen und die Funktionen der Geräte mithilfe von Konfigurationsprofilen beschränken. Sie können Konfigurationsprofile hinzufügen und ändern sowie Profile auf mobilen Geräten installieren.
- Apps mithilfe von Provisioning-Profilen nicht über den App Store auf mobilen Geräten installieren. Beispielsweise können Sie mithilfe von Provisioning-Profilen firmenintern entwickelte Unternehmens-Apps auf den mobilen Geräten der Benutzer installieren. Ein Provisioning-Profil enthält Informationen über die App und das mobile Gerät.
- Apps auf dem iOS MDM-Gerät über den App Store installieren. Vor der Installation der App auf dem iOS MDM-Gerät muss die App zum iOS MDM-Server hinzugefügt werden.

Sämtliche verbundenen iOS MDM-Geräte erhalten alle 24 Stunden PUSH-Benachrichtigungen zur Synchronisierung der Daten mit dem iOS MDM-Server.

Informationen über das Konfigurationsprofil und das Provisioning-Profil sowie über die auf dem iOS MDM-Gerät installierten Apps können im Fenster Geräteeigenschaften angezeigt werden.

Ein iOS MDM-Profil mittels Zertifikat signieren

Sie können ein iOS MDM-Profil unter Verwendung eines Zertifikats signieren. Sie können entweder eine Zertifikat verwenden, welches Sie selbst ausgestellt haben, oder welches Sie von einer vertrauenswürdigen Zertifizierungsstelle erhalten haben.

iOS-Geräte zeigen für nicht signierte Profile einen Hinweis an und fordern den Benutzer bei der Installation des Profils auf, dem Unterzeichner zu vertrauen.

So signieren Sie ein iOS MDM-Profil mittels eines Zertifikats:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Mobile Geräte**, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Ordners den Bereich **Verbindungseinstellungen für iOS-Geräte** aus.
4. Klicken Sie auf die Schaltfläche **Durchsuchen** unter dem Feld **Zertifikatdatei auswählen**.

   Das Fenster **Zertifikat**.

5. Wählen Sie im Feld **Zertifikatstyp** entweder einen offenen oder geschlossenen Zertifikatstyp aus:

   - Wenn der Wert **Container PKCS#12** ausgewählt ist, geben Sie die Zertifikatsdatei und das Kennwort an.
   - Wenn der Wert **X.509-Zertifikat** ausgewählt ist:

     a. Geben Sie die Datei des privaten Schlüssels an (Datei mit der Erweiterung *prk oder *.pem).

     b. Geben Sie das Kennwort des privaten Schlüssels an.

     c. Geben Sie die Datei des öffentlichen Schlüssels an (Datei mit der Erweiterung cer).

6. Klicken Sie auf die Schaltfläche **OK**.

Das iOS MDM-Profil ist mittels eines Zertifikats signiert.

Konfigurationsprofil hinzufügen

Zum Erstellen eines Konfigurationsprofils können Sie den Apple Configurator 2 verwenden, der auf der Internetseite von Apple Inc. verfügbar ist. Apple Configurator 2 funktioniert nur auf Geräten, auf denen macOS ausgeführt wird. Wenn Ihnen solche Geräte nicht zur Verfügung stehen, können Sie stattdessen das iPhone Configuration Utility auf einem Gerät mit Verwaltungskonsole verwenden. Allerdings wird das iPhone Configuration Utility von Apple Inc. nicht mehr unterstützt.

Um ein Konfigurationsprofil mittels iPhone Configuration Utility zu erstellen und es zum iOS MDM-Server hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Verwaltung mobiler Geräte** den Unterordner **Server für mobile Geräte** aus.
3. Wählen Sie im Arbeitsbereich des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.
4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Servers für mobile Geräte wird geöffnet.
5. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Konfigurationsprofile** aus.
6. Klicken Sie im Abschnitt **Konfigurationsprofile** auf die Schaltfläche **Erstellen**.

   Das Fenster **Neues Konfigurationsprofil** wird geöffnet.
7. Geben Sie im Fenster **Neues Konfigurationsprofil** den Namen des Profils sowie die ID des Profils an.

   Die Kennung des Konfigurationsprofils muss eindeutig sein. Der ID-Wert muss im Format Reverse-DNS angegeben werden (z. B. *com.companyname.identifier*).
8. Klicken Sie auf die Schaltfläche **OK**.

   Daraufhin wird das iPhone Configuration Utility gestartet, wenn Sie es installiert haben.

9. Passen Sie die Einstellungen des Profils mit dem Programm iPhone Configuration Utility an.

   Eine Beschreibung der Profileinstellungen und eine Konfigurationsanleitung finden Sie in der Dokumentation zum Programm iPhone Configuration Utility.

   Nachdem das Profil mit dem Programm iPhone Configuration Utility angepasst wurde, erscheint das neue Konfigurationsprofil im Abschnitt **Konfigurationsprofile** des Eigenschaftenfensters für den iOS MDM-Server.

   Das Konfigurationsprofil kann mithilfe der Schaltfläche **Ändern** bearbeitet werden.

   Mithilfe der Schaltfläche **Importieren** können Sie ein Konfigurationsprofil ins Programm laden.

   Konfigurationsprofile können mithilfe der Schaltfläche **Exportieren** in einer Datei gespeichert werden.

Das Profil, dass Sie erstellt haben, muss auf iOS MDM-Geräten installiert werden.

Konfigurationsprofil auf dem Gerät hinzufügen

Gehen Sie wie folgt vor, um ein Konfigurationsprofil auf einem mobilen Gerät zu installieren:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsbereich anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, auf dem das Konfigurationsprofil installiert werden soll.

   Sie können mehrere mobile Geräte auswählen und das Profil gleichzeitig darauf installieren.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

5. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt **Profil installieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Profil installieren** auswählen.

   Daraufhin wird das Fenster **Profile auswählen** mit der Profilliste geöffnet. Wählen Sie aus der Liste das Profil aus, das auf dem mobilen Gerät installiert werden soll. Sie können gleichzeitig mehrere Profile auswählen und auf dem mobilen Gerät installieren. Verwenden Sie die Taste **Umschalt**, um einen Bereich von mehreren Profilen auszuwählen. Um mehrere einzelne Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **Strg**.

6. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Konfigurationsprofil auf dem mobilen Gerät des Benutzers installiert. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls im Befehlsprotokoll auf *Ausgeführt*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

7. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung mobiler Geräte** zu schließen.

Sie können das von Ihnen installierte Profil und anzeigen und gegebenenfalls entfernen.

Konfigurationsprofil vom Gerät löschen

Um ein Konfigurationsprofil von einem mobilen Gerät zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsbereich mithilfe des Links **iOS MDM**.

3. Wählen Sie das mobile Gerät des Benutzers, von dem das Konfigurationsprofil gelöscht werden soll.

   Sie können mehrere mobile Geräte auswählen und das Profil gleichzeitig von diesen Geräten löschen.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

5. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt **Profil entfernen** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können auch einen Befehl an das mobile Gerät senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Profil entfernen** auswählen.

   Daraufhin wird das Fenster **Profile entfernen** mit der Profilliste geöffnet.

6. Wählen Sie aus der Liste das Profil aus, das vom mobilen Gerät gelöscht werden soll. Sie können gleichzeitig mehrere Profile auswählen und vom mobilen Gerät löschen. Verwenden Sie die Taste **Umschalt**, um einen Bereich von mehreren Profilen auszuwählen. Um mehrere einzelne Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **Strg**.

7. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Konfigurationsprofil vom mobilen Gerät des Benutzers gelöscht. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

8. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung mobiler Geräte** zu schließen.

Hinzufügen eines neuen Geräts mittels der Veröffentlichung eines Links auf das Profil

Der Administrator erstellt in der Verwaltungskonsole mithilfe des Assistent für die Installation eines Zertifikats ein neues iOS MDM-Profil. Als Ergebnis der Ausführung des Assistenten werden die folgenden Aktionen ausgeführt:

- Das iOS MDM-Profil wird automatisch auf dem Webserver veröffentlicht.
- Dem Benutzer wird in einer SMS-Nachricht oder per E-Mail ein Link auf das iOS MDM-Profil zugesendet. Nach dem Erhalten des Links installiert der Benutzer das iOS MDM-Profil auf dem mobilen Gerät.
- Daraufhin wird das mobile Gerät mit dem iOS MDM-Server verbunden.

In Zusammenhang mit der Verschärfung der Sicherheitsrichtlinie durch das Unternehmen Apple müssen für die Verbindung von mobilen Geräten mit dem Betriebssystem iOS 11 zum Administrationsserver mit eingerichteter PKI-Integration (Public Key Infrastructure) die Protokolle der Versionen TLS 1.1 und TLS 1.2 konfiguriert werden.

Hinzufügen eines neuen Geräts mittels der Installation des Profils durch den Administrator

Um eine Verbindung zwischen Mobilgerät und dem iOS MDM-Server mithilfe der Installation des iOS MDM-Profils auf dem mobilen Gerät herzustellen, muss der Administrator wie folgt vorgehen:

1. Öffnen Sie in Verwaltungskonsole den Assistent für die Installation eines Zertifikats.
2. Erstellen Sie ein neues iOS MDM-Profil durch Aktivieren des Kontrollkästchens **Zertifikat nach Fertigstellen des Assistenten anzeigen** im Fenster des Assistenten.
3. Das iOS MDM-Profil speichern.
4. Das iOS MDM-Profil auf dem mobilen Gerät des Benutzers mithilfe des Tools Apple Configurator installieren.

   Daraufhin wird das mobile Gerät mit dem iOS MDM-Server verbunden.

In Zusammenhang mit der Verschärfung der Sicherheitsrichtlinie durch das Unternehmen Apple müssen für die Verbindung von mobilen Geräten mit dem Betriebssystem iOS 11 zum Administrationsserver mit eingerichteter PKI-Integration (Public Key Infrastructure) die Protokolle der Versionen TLS 1.1 und TLS 1.2 konfiguriert werden.

Provisioning-Profil hinzufügen

Gehen Sie wie folgt vor, um ein Provisioning-Profil zum iOS MDM-Server hinzuzufügen:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte**.
2. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Server für mobile Geräte** aus.
3. Wählen Sie im Arbeitsbereich des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.

4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Servers für mobile Geräte wird geöffnet.

5. Wechseln Sie im Eigenschaftenfenster **des iOS MDM-Servers** zum Abschnitt **Provisioning-Profile**.

6. Klicken Sie im Abschnitt **Provisioning-Profile** auf die Schaltfläche **Importieren** und geben Sie den Pfad zur Datei des Provisioning-Profils an.

Das Profil wird zu den Einstellungen des iOS MDM-Servers hinzugefügt.

Provisioning-Profile können mithilfe der Schaltfläche **Exportieren** in einer Datei gespeichert werden.

Sie können das von Ihnen importierte Provisioning-Profil auf iOS MDM-Geräten installieren.

Provisioning-Profil auf dem Gerät installieren

Gehen Sie wie folgt vor, um ein Provisioning-Profil auf einem mobilen Gerät zu installieren:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsbereich anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, auf dem das Provisioning-Profil installiert werden soll.

   Sie können mehrere mobile Geräte auswählen und das Provisioning-Profil gleichzeitig darauf installieren.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

5. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt **Provisioning-Profil installieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Provisioning-Profil installieren** auswählen.

   Daraufhin wird das Fenster **Provisioning-Profile auswählen** mit der Liste der Provisioning-Profile geöffnet. Wählen Sie aus der Liste das Provisioning-Profil aus, das auf dem mobilen Gerät installiert werden soll. Sie können gleichzeitig mehrere Provisioning-Profile auswählen und auf dem mobilen Gerät installieren. Verwenden Sie die Taste **Umschalt**, um einen Bereich von mehreren Provisioning-Profilen auszuwählen. Um mehrere einzelne Provisioning-Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **Strg**.

6. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Provisioning-Profil auf dem mobilen Gerät des Benutzers installiert. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls im Befehlsprotokoll auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

7. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung mobiler Geräte** zu schließen.

Sie können das von Ihnen installierte Profil und anzeigen und gegebenenfalls entfernen.

Provisioning-Profil vom Gerät löschen

Um ein Provisioning-Profil von einem mobilen Gerät zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsbereich anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, von dem das Provisioning-Profil gelöscht werden soll.

   Sie können mehrere mobile Geräte auswählen und das Provisioning-Profil gleichzeitig von diesen Geräten löschen.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

5. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt **Provisioning-Profil entfernen** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können auch einen Befehl an das mobile Gerät senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Provisioning-Profil entfernen** auswählen.

   Daraufhin wird das Fenster **Provisioning-Profile entfernen** mit der Profilliste geöffnet.

6. Wählen Sie aus der Liste das Provisioning-Profil aus, das vom mobilen Gerät gelöscht werden soll. Sie können gleichzeitig mehrere Provisioning-Profile auswählen und vom mobilen Gerät löschen. Verwenden Sie die Taste **Umschalt**, um einen Bereich von mehreren Provisioning-Profilen auszuwählen. Um mehrere einzelne Provisioning-Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **Strg**.

7. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Provisioning-Profil vom mobilen Gerät des Benutzers gelöscht. Apps, die mit dem gelöschten Provisioning-Profil verknüpft sind, funktionieren dann nicht mehr. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

8. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung mobiler Geräte** zu schließen.

Verwaltete Apps hinzufügen

Vor der Installation der App auf dem iOS MDM-Gerät muss die App zum iOS MDM-Server hinzugefügt werden. Eine App wird verwaltet, wenn sie mithilfe von Kaspersky Security Center auf dem Gerät installiert wurde. Eine verwaltete App kann mithilfe von Kaspersky Security Center ferngesteuert verwaltet werden.

Gehen Sie wie folgt vor, um eine verwaltete App zum iOS MDM-Server hinzuzufügen:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte**.
2. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Server für mobile Geräte** aus.
3. Wählen Sie im Arbeitsbereich des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.
4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des iOS MDM-Servers wird geöffnet.
5. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Verwaltete Programme** aus.
6. Klicken Sie im Abschnitt **Verwaltete Programme** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Programm hinzufügen** wird geöffnet.
7. Geben Sie im Fenster **Programm hinzufügen** im Feld **App-Name** den Namen der hinzugefügten App ein.
8. Geben Sie im Feld **Apple ID oder Link zur Manifest-Datei** die Apple ID der hinzugefügten App oder den Link zur Manifestdatei an, über den die App heruntergeladen werden kann.
9. Wenn Sie möchten, dass beim Löschen des iOS MDM-Profils gleichzeitig mit dem Profil auch die verwaltete App vom mobilen Gerät des Benutzers gelöscht wird, aktivieren Sie das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren**.
10. Wenn Sie die Daten-Backups der Anwendung durch iTunes verbieten möchten, aktivieren Sie das Kontrollkästchen **Erstellen von Backup-Kopien der Daten verbieten**.
11. Klicken Sie auf die Schaltfläche **OK**.

Die hinzugefügte App wird im Abschnitt **Verwaltete Programme** des Eigenschaftenfensters des iOS MDM-Servers angezeigt.

App auf dem mobilen Gerät installieren

Gehen Sie wie folgt vor, um eine App auf einem mobilen iOS MDM-Gerät zu installieren:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.
2. Wählen Sie das iOS MDM-Gerät, auf dem die App installiert werden soll.

   Sie können mehrere mobile Geräte auswählen und die App gleichzeitig darauf installieren.
3. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.
4. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt **App installieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **App installieren** auswählen.

Daraufhin wird das Fenster **Apps zur Installation auswählen** mit der Profilliste geöffnet. Wählen Sie aus der Liste die App aus, die auf dem mobilen Gerät installiert werden soll. Sie können gleichzeitig mehrere Apps auswählen und auf dem mobilen Gerät installieren. Verwenden Sie die Taste **Umschalt**, um einen Bereich von mehreren Apps auszuwählen. Um mehrere einzelne Apps zu einer Gruppe zusammenzufügen verwenden Sie die Taste **Strg**.

5. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird die ausgewählte App auf dem mobilen Gerät des Benutzers installiert. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls im Befehlsprotokoll auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden. Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

6. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung mobiler Geräte** zu schließen.

Informationen über die installierte App werden in den Eigenschaften des mobilen iOS MDM-Geräts angezeigt. Sie können die App mithilfe des Befehlsprotokolls oder aus dem Kontextmenü des mobilen Geräts löschen.

App vom Gerät löschen

Um eine App von einem mobilen Gerät zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsbereich anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, von dem die App gelöscht werden soll.

   Sie können mehrere mobile Geräte auswählen und die App gleichzeitig von diesen Geräten löschen.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

5. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt **App löschen** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **App löschen** auswählen.

   Daraufhin wird das Fenster **Apps entfernen** mit einer Liste der Anwendungen geöffnet.

6. Wählen Sie aus der Liste die App aus, die vom mobilen Gerät gelöscht werden soll. Sie können gleichzeitig mehrere Apps auswählen und vom Gerät löschen. Verwenden Sie die Taste **Umschalt**, um einen Bereich von mehreren Apps auszuwählen. Um mehrere einzelne Apps zu einer Gruppe zusammenzufügen verwenden Sie die Taste **Strg**.

7. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird die ausgewählte App vom mobilen Gerät des Benutzers gelöscht. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

8. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung mobiler Geräte** zu schließen.

Roaming-Einstellungen auf einem mobilen iOS MDM-Gerät konfigurieren

Um die Roaming-Einstellungen zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltung mobiler Geräte**.
2. Wählen Sie im Ordner **Verwaltung mobiler Geräte** den Unterorder **Mobile Geräte**.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.
3. Wählen Sie das iOS MDM-Gerät des Benutzers, für welches Sie die Roaming-Einstellungen konfigurieren möchten.

   Sie können mehrere mobile Geräte auswählen und deren Roaming-Einstellungen gleichzeitig konfigurieren.
4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.
5. Wechseln Sie im Fenster **Befehle zur Verwaltung mobiler Geräte** zum Abschnitt **Roaming-Einstellungen konfigurieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können auch einen Befehl an das mobile Gerät senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle → Roaming konfigurieren** auswählen.
6. Geben Sie im Fenster **Roaming-Einstellungen** die erforderlichen Einstellungen an:

   - **Datenroaming aktivieren**

     Ist diese Option aktiviert, wird das Daten-Roaming auf dem mobilen iOS MDM-Gerät aktiviert. Der Benutzer des mobilen iOS MDM-Geräts kann das Internet mit Roaming nutzen.

     Diese Option ist standardmäßig deaktiviert.

Die Roaming-Einstellungen werden für die ausgewählten Geräte konfiguriert.

Informationen über das iOS MDM-Gerät anzeigen

Gehen Sie folgendermaßen vor, um Informationen über ein iOS MDM-Gerät anzuzeigen:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.
2. Filtern Sie die iOS MDM-Geräte im Arbeitsbereich mithilfe des Links **iOS MDM**.
3. Wählen Sie das mobile Gerät, für welches Sie die Informationen anzeigen wollen.

4. Klicken Sie mit der rechten Maustaste auf das gewünschte mobile Gerät und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster des iOS MDM-Geräts geöffnet.

Im Eigenschaftenfenster des mobilen Geräts werden Informationen über das angeschlossene iOS MDM-Gerät angezeigt.

Ausschluss eines iOS MDM-Geräts von der Verwaltung

Um ein iOS MDM-Gerät vom iOS MDM-Server auszuschließen, gehen Sie folgendermaßen vor:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsbereich mithilfe des Links **iOS MDM**.

3. Wählen Sie das mobile Gerät aus, das ausgeschlossen werden soll.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Löschen** aus.

   Daraufhin wird das iOS MDM-Gerät in der Liste zum Löschen markiert. Nachdem das mobile Gerät aus den Datenbanken des iOS MDM-Servers gelöscht wurde, wird es automatisch aus der Liste der verwalteten Geräte gelöscht. Für das Löschen des mobilen Geräts aus den Datenbanken des iOS MDM-Servers wird etwa eine Minute benötigt.

Als Folge des Ausschlusses eines iOS MDM-Geräts von der Verwaltung werden alle installierten Konfigurationsprofile, iOS MDM-Profile und Apps, für welche die Option **Zusammen mit dem iOS MDM-Profil deinstallieren** aktiviert wurde, vom mobilen Gerät gelöscht.

Senden von Befehlen an ein Gerät

So senden Sie einen Befehl an ein iOS MDM-Gerät:

1. Öffnen Sie in der Verwaltungskonsole den Knoten **Verwaltung mobiler Geräte**.

2. Wählen Sie den Ordner **Mobile Geräte** aus.

3. Im Ordner **Mobile Geräte** das mobile Gerät auswählen, an das Befehle gesendet werden sollen.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

5. Wählen Sie in der daraufhin angezeigten Liste den Befehl aus, der an das mobile Gerät gesendet werden soll.

Untersuchung des Ausführungsstatus der gesendeten Befehle

So überprüfen Sie den Ausführungsstatus eines Befehls, der an ein mobiles Gerät gesendet wurde:

1. Öffnen Sie in der Verwaltungskonsole den Knoten **Verwaltung mobiler Geräte**.

2. Wählen Sie den Ordner **Mobile Geräte** aus.

3. Im Ordner **Mobile Geräte** das mobile Gerät auswählen, auf dem der Ausführungsstatus der gesendeten Befehle geprüft werden soll.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Befehlsprotokoll anzeigen** aus.

KES-Geräte verwalten

In Kaspersky Security Center können Sie mobile KES-Geräte auf folgende Arten verwalten:

- KES-Geräte mithilfe von Befehlen zentral verwalten.
- Informationen über die Einstellungen für die Verwaltung von KES-Geräten anzeigen.
- Apps mithilfe von Paketen mit mobilen Apps installieren.
- KES-Geräte von der Verwaltung ausschließen.

Paket mit mobilen Anwendungen für KES-Geräte erstellen

Für die Erstellung eines Pakets mit mobilen Anwendungen ist für KES-Geräte eine Lizenz für Kaspersky Endpoint Security für Android erforderlich.

Gehen Sie wie folgt vor, um ein Paket für mobile Anwendungen zu erstellen:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.

   Der Ordner **Remote-Installation** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Klicken Sie auf die Schaltfläche **Weitere Aktionen** und wählen Sie **App-Pakete für mobile Geräte verwalten** in der Dropdown-Liste.

3. Klicken Sie im Fenster **App-Pakete für mobile Geräte verwalten** auf **Neu**.

4. Der Assistent für das Erstellen eines Installationspakets wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Das erstellte Paket mit mobilen Anwendungen wird im Fenster **App-Pakete für mobile Geräte verwalten** angezeigt.

Zertifikatbasierte Authentifizierung von KES-Geräten aktivieren

So aktivieren Sie die zertifikatbasierte Authentifizierung eines KES-Geräts:

1. Öffnen Sie die Systemregistrierung des Client-Geräts, auf dem der Administrationsserver installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** → **Ausführen**.

2. Rufen Sie den folgenden Abschnitt auf:

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM.

- Für 64-Bit-Systeme:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Erstellen Sie einen Schlüssel mit dem Namen "LP_MobileMustUseTwoWayAuthOnPort13292".
4. Geben Sie als Schlüsseltyp "REG_DWORD" an.
5. Legen Sie den Wert des Schlüssels mit 1 fest.
6. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin wird nach dem Start des Dienstes des Administrationsservers die verpflichtende zertifikatbasierte Authentifikation des KES-Gerätes unter Verwendung des allgemeinen Zertifikats aktiviert.

> Bei der ersten Verbindung des KES-Geräts mit dem Administrationsserver muss das Zertifikat nicht verpflichtend vorhanden sein.

Die zertifikatbasierte Authentifikation von KES-Geräten ist standardmäßig deaktiviert.

Informationen über das KES-Gerät anzeigen

Gehen Sie folgendermaßen vor, um Informationen über ein KES-Gerät anzuzeigen:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.
   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.
2. Filtern Sie die KES-Geräte im Arbeitsbereich nach dem Verwaltungsprotokoll *KES*.
3. Wählen Sie das mobile Gerät, für welches Sie die Informationen anzeigen wollen.
4. Klicken Sie mit der rechten Maustaste auf das gewünschte mobile Gerät und wählen Sie **Eigenschaften** aus.

Das Eigenschaftenfenster des KES-Geräts wird geöffnet.

Im Eigenschaftenfenster des mobilen Geräts werden Informationen über das angeschlossene KES-Gerät angezeigt.

Ein KES-Gerät von der Verwaltung ausschließen

Um ein KES-Gerät von der Verwaltung auszuschließen, muss der Benutzer den Administrationsagenten vom mobilen Gerät löschen. Nach dem Löschen des Administrationsagenten durch den Benutzer werden die Informationen über das mobile Gerät aus der Administrationsserver-Datenbank gelöscht. Anschließend kann der Administrator das Gerät aus der Liste der verwalteten Geräte löschen.

Gehen Sie folgendermaßen vor, um ein KES-Gerät aus der Liste der verwalteten Geräte zu löschen:

1. Wählen Sie im Ordner **Verwaltung mobiler Geräte** in der Konsolenstruktur den Unterordner **Mobile Geräte** aus.
   Im Arbeitsbereich des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die KES-Geräte im Arbeitsbereich nach dem Verwaltungsprotokoll *KES*.

3. Wählen Sie das mobile Gerät aus, das Sie aus der Verwaltung nehmen möchten.

4. Wählen Sie im Kontextmenü des mobilen Gerätes den Punkt **Löschen** aus.

Daraufhin wird das mobile Gerät aus der Liste der verwalteten Geräte gelöscht.

Wenn Kaspersky Endpoint Security für Android nicht vom mobilen Gerät gelöscht wird, erscheint das Gerät nach der Synchronisierung mit dem Administrationsserver wieder in der Liste der verwalteten Geräte.

Verschlüsselung und Datenschutz

Die Datenverschlüsselung senkt das Risiko eines unbeabsichtigten Informationsverlustes im Falle des Diebstahls oder Verlustes eines tragbaren Geräts, eines Wechselmediums oder einer Festplatte, oder beim Zugriff nicht autorisierter Benutzer und Programme auf Daten.

Die Verschlüsselungsfunktion ist im Programm Kaspersky Endpoint Security für Windows implementiert. Kaspersky Endpoint Security für Windows ermöglicht die Verschlüsselung von Dateien, die auf den lokalen Festplatten eines Geräts oder auf Wechseldatenträgern gespeichert sind, sowie die Verschlüsselung von ganzen Wechseldatenträgern und Festplatten.

Eine Konfiguration der Verschlüsselungsregeln erfolgt mit Kaspersky Security Center durch das Festlegen von Richtlinien. Die Verschlüsselung und Entschlüsselung nach den festgelegten Regeln erfolgen bei der Anwendung einer Richtlinie.

Die Verfügbarkeit der Funktionen zur Verschlüsselungsverwaltung wird durch die Einstellungen der Benutzeroberfläche bestimmt.

Der Administrator kann folgende Aktionen ausführen:

- Verschlüsselung oder Entschlüsselung von Dateien auf den lokalen Laufwerken eines Geräts anpassen.
- Verschlüsselung von Dateien auf Wechseldatenträgern konfigurieren und durchführen.
- Regeln für den Zugriff von Programmen auf verschlüsselte Dateien erstellen.
- Schlüsseldatei für den Zugriff auf verschlüsselte Dateien erstellen und an den Benutzer weitergeben, wenn die Verschlüsselungsfunktion für Dateien auf dem Gerät des Benutzers beschränkt wurde.
- Verschlüsselung von Festplatten anpassen und durchführen.
- Zugriff von Benutzern auf verschlüsselte Festplatten und Wechseldatenträger verwalten (Benutzerkonten des Authentifizierungsagenten verwalten, Antworten auf Anfragen zum Wiederherstellen des Benutzernamens und -kennworts sowie Zugriffsschlüssel auf verschlüsselte Geräte erstellen und an Benutzer weitergeben).
- Verschlüsselungsstatusmeldungen und Berichte über die Verschlüsselung von Dateien anzeigen.

Diese Vorgänge werden durch das Programm Kaspersky Endpoint Security für Windows ausgeführt. Ausführliche Anweisungen zur Ausführung der Vorgänge und eine Beschreibung der Besonderheiten der Verschlüsselungsfunktion können Sie der Online-Hilfe für Kaspersky Endpoint Security für Windows entnehmen.

Kaspersky Security Center unterstützt die Funktionen Verschlüsselungsverwaltung für Geräte mit den Betriebssystemen macOS. Die Verschlüsselungseinstellungen werden mithilfe des Programms Kaspersky Endpoint Security for Mac für jene Programmversionen ausgeführt, in denen die Verschlüsselungsfunktion unterstützt wird. Ausführliche Anweisungen zur Ausführung der Vorgänge und eine Beschreibung der Besonderheiten der Verschlüsselungsfunktion können Sie dem *Administratorhandbuch für Kaspersky Endpoint Security for Mac* entnehmen.

Liste der verschlüsselten Geräte anzeigen

Um sich eine Liste der Geräte anzeigen zu lassen, deren Informationen verschlüsselt wurden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur des Administrationsservers den Ordner **Verschlüsselung und Datenschutz**.
2. Wechseln Sie in die Liste der verschlüsselten Geräte auf eine der folgenden Arten:
   - Klicken Sie auf den Link **Zur Liste der verschlüsselten Laufwerke** im Abschnitt **Verschlüsselte Laufwerke verwalten**.
   - Wählen Sie in der Konsolenstruktur den Unterordner **Verschlüsselte Laufwerke** aus.

Daraufhin werden im Arbeitsbereich Informationen über die im Netzwerk vorhandenen Geräte, auf denen verschlüsselte Dateien vorhanden sind, angezeigt, sowie die Geräte, die auf der Ebene der Festplatten verschlüsselt wurden. Nachdem die Informationen auf einem Gerät entschlüsselt wurden, wird das Gerät automatisch aus der Liste entfernt.

Sie können die Informationen in der Geräteliste nach einer beliebigen Spalte in auf- oder absteigender Reihenfolge sortieren.

Ob der Ordner **Verschlüsselung und Datenschutz** in der Konsolenstruktur vorhanden ist, wird durch die Einstellungen der Benutzeroberfläche definiert.

Liste der Verschlüsselungsereignisse anzeigen

Bei der Ausführung der Aufgaben zur Datenverschlüsselung oder -entschlüsselung auf den Client-Geräten sendet Kaspersky Endpoint Security für Windows an Kaspersky Security Center Informationen über aufgetretene Ereignisse folgender Typen:

- Eine Datei kann nicht verschlüsselt oder entschlüsselt oder ein verschlüsseltes Archiv kann wegen zu wenig Speicherplatz auf der Festplatte nicht erstellt werden.
- Eine Datei kann nicht verschlüsselt oder entschlüsselt oder ein verschlüsseltes Archiv kann aufgrund eines Problems mit der Lizenz nicht erstellt werden.
- Eine Datei kann nicht verschlüsselt oder entschlüsselt oder ein verschlüsseltes Archiv kann wegen fehlender Zugriffsrechte nicht erstellt werden.
- Der Zugriff eines Programms auf eine verschlüsselte Datei wurde verweigert.
- Unbekannte Fehler.

Um sich eine Liste der Ereignisse anzeigen zu lassen, die bei einer Datenverschlüsselung auf Client-Geräten aufgetreten sind, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur des Administrationsservers den Ordner **Verschlüsselung und Datenschutz**.
2. Wechseln Sie in die Liste der Ereignisse, die bei der Datenverschlüsselung aufgetreten sind, auf eine der folgenden Arten:
   - Klicken Sie auf den Link **Zur Fehlerliste wechseln** im Abschnitt **Fehler bei Datenverschlüsselung**.
   - Wählen Sie in der Konsolenstruktur den Unterordner **Verschlüsselte Laufwerke** aus.

Daraufhin werden im Arbeitsbereich Informationen über die Probleme angezeigt, die bei der Datenverschlüsselung auf den Client-Geräten aufgetreten sind.

Sie können folgende Aktionen auf die Liste der Verschlüsselungsereignisse anwenden:

- Einträge in jeder Spalte aufsteigend oder absteigend sortieren
- schnelle Suche nach Einträgen ausführen (nach einer Textübereinstimmung mit der Teilzeichenfolge in einem beliebigen Listenfeld)
- die erstellte Ereignisliste in eine Textdatei exportieren

Ob der Ordner **Verschlüsselung und Datenschutz** in der Konsolenstruktur vorhanden ist, wird durch die Einstellungen der Benutzeroberfläche definiert.

Liste der Verschlüsselungsereignisse in eine Textdatei exportieren

Um eine Liste der Verschlüsselungsereignisse in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Erstellen Sie eine Liste der Verschlüsselungsereignisse.
2. Klicken Sie mit der rechten Maustaste auf die Ereignisliste und wählen Sie **Liste exportieren**.

   Das Fenster **Liste exportieren** wird geöffnet.
3. Geben Sie im Fenster **Liste exportieren** den Namen der Textdatei mit der Ereignisliste ein, wählen einen Ordner, in dem die Datei gespeichert werden soll, und klicken Sie auf die Schaltfläche **Speichern**.

   Die Liste der Verschlüsselungsereignisse wird in der angegebenen Datei gespeichert.

Verschlüsselungsberichte erstellen und anzeigen

Sie können folgende Berichte erstellen:

- Bericht über den Verschlüsselungsstatus verwalteter Geräte. Dieser Bericht enthält Details zur Datenverschlüsselung verschiedener verwalteter Geräte. Der Bericht zeigt beispielsweise die Anzahl der Geräte, für welche die Richtlinie mit konfigurierten Verschlüsselungsregeln gilt. Außerdem können Sie ihm entnehmen, wie viele Geräte neu gestartet werden müssen. Darüber hinaus enthält der Bericht Informationen über die Verschlüsselungstechnologie und den Algorithmus für jedes Gerät.

- Bericht über den Verschlüsselungsstatus der Massenspeichergeräte. Dieser Bericht enthält ähnliche Informationen wie der Bericht zum Verschlüsselungsstatus verwalteter Geräte, verfügt aber lediglich über Informationen zu Massenspeichergeräten und Wechseldatenträgern.

- Bericht über Zugriffsrechte auf verschlüsselte Laufwerke. Dieser Bericht zeigt, welche Benutzerkonten Zugriff auf verschlüsselte Laufwerke haben.

- Bericht über Fehler bei der Dateiverschlüsselung. Dieser Bericht enthält Informationen über Fehler, die bei der Ausführung der Aufgaben zur Verschlüsselung und Entschlüsselung von Daten auf den Client-Geräten aufgetreten sind.

- Bericht über blockierte Zugriffe auf verschlüsselte Dateien. Dieser Bericht enthält Informationen über das Blockieren des Zugriffs von Anwendungen auf verschlüsselte Dateien. Dieser Bericht ist hilfreich, wenn nicht autorisierte Benutzer oder Programme versuchen, auf verschlüsselte Dateien oder Laufwerke zuzugreifen.

Um den Bericht über die Verschlüsselung von Geräten zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verschlüsselung und Datenschutz** aus.

2. Führen Sie eine der folgenden Aktionen aus:

   - Um einen Bericht über den Verschlüsselungsstatus verwalteter Geräte zu erstellen, klicken Sie auf den Link **Bericht über den Verschlüsselungsstatus der Massenspeichergeräte anzeigen**.

     Wenn Sie diesen Bericht noch nicht konfiguriert haben, wird der Assistent für das Erstellen einer Berichtsvorlage gestartet. Folgen Sie den Schritten des Assistenten.

   - Um einen Bericht über den Verschlüsselungsstatus von Massenspeichergeräten zu erstellen, wählen Sie in der Konsolenstruktur den Unterordner **Verschlüsselte Laufwerke** aus und klicken Sie dann auf **Bericht über den Verschlüsselungsstatus der Massenspeichergeräte anzeigen**.

Die Erstellung des Berichts wird gestartet. Der Bericht wird auf der Registerkarte **Berichte** des Knotens **Administrationsserver** angezeigt.

Um den Bericht über die Zugriffsberechtigungen für verschlüsselte Geräte zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verschlüsselung und Datenschutz** aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf den Link **Bericht über Zugriffsrechte auf verschlüsselte Laufwerke** im Abschnitt **Verschlüsselte Laufwerke verwalten**, um den "Assistenten für das Erstellen einer Berichtsvorlage" zu starten.
   - Wählen Sie den Unterordner **Verschlüsselte Laufwerke** aus und klicken Sie dann auf **Bericht über Zugriffsrechte auf verschlüsselte Laufwerke**, um den "Assistenten für das Erstellen einer Berichtsvorlage" zu starten.
3. Folgen Sie dem Assistenten für das Erstellen einer Berichtsvorlage.

Die Erstellung des Berichts wird gestartet. Der Bericht wird auf der Registerkarte **Berichte** des Knotens **Administrationsserver** angezeigt.

Um den Bericht über Fehler bei der Dateiverschlüsselung zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verschlüsselung und Datenschutz** aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf den Link **Bericht über Fehler bei der Dateiverschlüsselung anzeigen** im Abschnitt **Fehler bei der Datenverschlüsselung**, um den "Assistenten für das Erstellen einer Berichtsvorlage" zu starten.
   - Wählen Sie den Unterordner **Verschlüsselungsereignisse**, und starten Sie durch Klicken auf den Link **Bericht über Fehler bei der Dateiverschlüsselung** den Assistenten für das Erstellen einer Berichtsvorlage.
3. Folgen Sie dem Assistenten für das Erstellen einer Berichtsvorlage.

Die Erstellung des Berichts wird gestartet. Der Bericht wird auf der Registerkarte **Berichte** des Knotens **Administrationsserver** angezeigt.

Um dem Bericht über den Verschlüsselungsstatus der verwalteten Geräte zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.
3. Starten Sie über die Schaltfläche **Neue Berichtsvorlage** den Assistenten für das Erstellen einer Berichtsvorlage.

4. Folgen Sie den Anweisungen des Assistenten für das Erstellen einer Berichtsvorlage. Wählen Sie im Fenster **Typ der Berichtsvorlage auswählen** im Abschnitt **Andere** den Punkt **Bericht über den Verschlüsselungsstatus verwalteter Geräte** aus.

   Nach Fertigstellen des Assistenten für das Erstellen einer Berichtsvorlage wird im Knoten Administrationsserver auf der Registerkarte **Berichte** die erstellte Berichtsvorlage angezeigt.

5. Wählen Sie im Knoten des benötigten Administrationsservers auf der Registerkarte **Berichte** die Vorlage für den Bericht, der in den vorherigen Schritten der Anleitung erstellt wurde.

Die Erstellung des Berichts wird gestartet. Der Bericht wird auf der Registerkarte **Berichte** des Knotens **Administrationsserver** angezeigt.

Informationen darüber, ob der Verschlüsselungsstatus der Geräte und Wechseldatenträger der Verschlüsselungsrichtlinie entspricht, können Sie in den Informationsbereichen auf der Registerkarte **Statistik** im Knoten Administrationsserver anzeigen lassen.

Um den Bericht über blockierte Zugriffe auf verschlüsselte Dateien zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

2. Wählen Sie im Arbeitsbereich des Knotens die Registerkarte **Berichte** aus.

3. Klicken Sie auf die Schaltfläche **Neue Berichtsvorlage**, um den "Assistenten für das Erstellen einer Berichtsvorlage" zu starten.

4. Folgen Sie den Anweisungen des Assistenten für das Erstellen einer Berichtsvorlage. Wählen Sie im Fenster **Typ der Berichtsvorlage auswählen** im Abschnitt **Andere** den Punkt **Bericht über blockierte Zugriffe auf verschlüsselte Dateien** aus.

   Nachdem der Assistent für das Erstellen einer Berichtsvorlage beendet ist, wird im Knoten **Administrationsserver** auf der Registerkarte **Berichte** eine neue Berichtsvorlage angezeigt.

5. Wählen Sie im Knoten **Administrationsserver** auf der Registerkarte **Berichte** die Vorlage für den Bericht, der in den vorherigen Schritten der Anleitung erstellt wurde.

Die Erstellung des Berichts wird gestartet. Der Bericht wird auf der Registerkarte **Berichte** des Knotens **Administrationsserver** angezeigt.

Übertragung von Chiffrierschlüsseln zwischen Administrationsservern

Wenn die Datenverschlüsselungsfunktion auf einem verwalteten Gerät aktiviert ist, so ist der Chiffrierschlüssel auf dem Administrationsserver gespeichert. Der Chiffrierschlüssel wird verwendet, um auf verschlüsselte Daten zuzugreifen und um die Verschlüsselungsrichtlinie zu verwalten.

Der Chiffrierschlüssel muss in folgenden Fällen an einen anderen Administrationsserver übertragen werden:

- Sie konfigurieren den Administrationsagenten auf einem verwalteten Gerät neu, um das Gerät einem anderen Administrationsserver zuzuweisen. Wenn dieses Gerät verschlüsselte Daten enthält, muss der Chiffrierschlüssel an den Ziel-Administrationsserver übertragen werden. Andernfalls können die Daten nicht entschlüsselt werden.

- Sie verschlüsseln ein Wechseldatenträger, der mit einem vom Administrationsserver S1 verwalteten Gerät G1 verbunden ist, und verbinden diesen Wechseldatenträger mit einem vom Administrationsserver S2 verwalteten Gerät G2. Um auf die Daten des Wechseldatenträgers zugreifen zu können, muss der Chiffrierschlüssel von Administrationsserver S1 zu Administrationsserver S2 übertragen werden.

- Sie verschlüsseln eine Datei auf einem Gerät G1, das vom Administrationsserver S1 verwaltet wird, und versuchen dann, auf die Datei auf einem Gerät G2 zuzugreifen, das vom Administrationsserver S2 verwaltet wird. Um auf die Datei zugreifen zu können, muss der Chiffrierschlüssel von Administrationsserver S1 zu Administrationsserver S2 übertragen werden.

Sie können Chiffrierschlüssel wie folgt übertragen:

- Automatisch durch Aktivieren der Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen** in den Eigenschaften von zwei Administrationsservern, zwischen denen ein Chiffrierschlüssel übertragen werden muss. Wenn diese Option für einen der Administrationsserver deaktiviert ist, so ist die automatische Übertragung von Chiffrierschlüsseln nicht möglich.

  Wenn Sie in den Einstellungen des Administrationsservers die Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen** aktivieren, sendet der Administrationsserver sämtliche, in seiner Datenverwaltung befindliche, Chiffrierschlüssel an den primären Administration Server (falls vorhanden) der nächsthöheren Hierarchie-Ebene.

  Wenn Sie versuchen, auf verschlüsselte Daten zuzugreifen, durchsucht der Administrationsserver zuerst die Chiffrierschlüssel in seiner eigenen Datenverwaltung. Wenn die Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen** aktiviert ist und der erforderliche Chiffrierschlüssel nicht in der Datenverwaltung gefunden wurde, sendet der Administrationsserver zusätzlich eine Anfrage an die primären Administrationsserver (falls vorhanden), damit der erforderliche Chiffrierschlüssel bereitgestellt wird. Die Anfrage wird an alle primären Administrationsserver bis zum Server auf der höchsten Hierarchie-Ebene gesendet.

Die Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen**, ist derzeit in der Benutzeroberfläche von Web Console nicht verfügbar. Wenn Sie keinen Zugriff auf die MMC-basierte Verwaltungskonsole haben, verwenden Sie den primären Administrationsserver, um verschlüsselte Geräte zu verwalten.

- Manuell von einem Administrationsserver zu einem anderen durch den Export und Import einer Datei mit den Verschlüsselungsschlüsseln.

  Der Export und Import von Chiffrierschlüsseln sind Vorgänge, die in der Verwaltungsfunktion für Chiffrierschlüssel enthalten sind. Um diese Vorgänge auszuführen, Konfigurieren Sie die Zugriffsrechte auf die Funktion für Benutzer von Kaspersky Security Center wie folgt:

  - Gewähren Sie für einen Benutzer, der Chiffrierschlüssel vom sekundärer Administrationsserver exportiert die Zugriffsberechtigung auf die Verwaltungsfunktion für Chiffrierschlüssel **Lesen**.

  - Gewähren Sie für einen Benutzer, der Chiffrierschlüssel in den sekundären Ziel-Administrationsserver importiert die Zugriffsberechtigung auf die Verwaltungsfunktion für Chiffrierschlüssel **Schreiben**.

Um die automatische Übertragung von Chiffrierschlüsseln zwischen Administrationsservern innerhalb der Hierarchie zu aktivieren:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den die automatische Übertragung von Chiffrierschlüsseln aktiviert werden soll.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster den Abschnitt **Verschlüsselungsalgorithmus** aus.
4. Aktivieren Sie die Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen**.
5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.

Die Chiffrierschlüssel werden bei der nächsten Synchronisierung (Heartbeat) an die primären Administrationsserver (falls vorhanden) übertragen. Dieser Administrationsserver stellt auch auf Anfrage einen Chiffrierschlüssel aus seiner Datenverwaltung für einen sekundären Administrationsserver bereit.

Um die Chiffrierschlüssel manuell zwischen Administrationsservern zu übertragen:

1. Wählen Sie in der Konsolenstruktur des Administrationsservers den sekundären Administrationsserver aus, von dem Sie die Verschlüsselungsschlüssel übertragen möchten.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster den Abschnitt **Verschlüsselungsalgorithmus** aus.
4. Klicken Sie auf **Chiffrierschlüssel von Administrationsserver exportieren**.

   Stellen Sie sicher, dass einem Benutzer, der Chiffrierschlüssel vom Server exportiert, die Zugriffsberechtigung auf die Verwaltungsfunktion für Chiffrierschlüssel **Lesen** gewährt wurde.
5. Im Fenster **Chiffrierschlüssel exportieren**:
   - Klicken Sie auf **Durchsuchen** und geben Sie dann an, wo die Datei gespeichert werden soll.
   - Geben Sie ein Kennwort an, um die Datei vor unbefugtem Zugriff zu schützen.

     Merken Sie sich das Kennwort. Ein verlorenes Kennwort kann nicht wiederhergestellt werden. Wenn das Kennwort verloren geht, müssen Sie den Exportvorgang wiederholen. Notieren Sie sich daher das Kennwort und habe Sie es griffbereit.
6. Übertragen Sie die Datei auf einen anderen Administrationsserver, z. B. über einen freigegebenen Ordner oder einen Wechseldatenträger.
7. Stellen Sie sicher, dass auf dem Ziel-Administrationsserver die Kaspersky Security Center Verwaltungskonsole ausgeführt wird.
8. Wählen Sie in der Konsolenstruktur des Administrationsservers den Zieladministrationsserver aus, auf den Sie die Verschlüsselungsschlüssel übertragen möchten.
9. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
10. Wählen Sie im Eigenschaftenfenster den Abschnitt **Verschlüsselungsalgorithmus** aus.

11. Klicken Sie auf die Schaltfläche **Chiffrierschlüssel in Administrationsserver importieren**.

    Stellen Sie sicher, dass einem Benutzer, der Chiffrierschlüssel auf einem Server importiert, die Zugriffsberechtigung auf die Verwaltungsfunktion für Chiffrierschlüssel **Schreiben** gewährt wurde.

12. Im Fenster **Importiere Chiffrierschlüssel**:

    - Klicken Sie auf **Durchsuchen** und wählen Sie dann die Datei mit den Chiffrierschlüsseln aus.
    - Geben Sie das Kennwort an.

13. Klicken Sie auf die Schaltfläche **OK**.

Die Chiffrierschlüssel werden an den Zieladministrationsserver übertragen.

Datenverwaltung

Dieser Abschnitt enthält Informationen zu Daten, die auf dem Administrationsserver gespeichert und zur Überwachung und Wartung von Client-Geräten verwendet werden.

Die zur Statusverfolgung der Client-Geräte und deren Wartung verwendeten Daten werden in der Konsolenstruktur im Ordner **Datenverwaltung** angezeigt.

Der Ordner **Datenverwaltung** enthält die folgenden Objekte:

- Durch den Administrationsserver heruntergeladene Updates, die auf Client-Geräte verteilt werden
- Liste der im Netzwerk gefundenen Hardware
- Auf den Client-Geräten gefundene Lizenzschlüssel
- Dateien, die von Sicherheitsanwendungen in den Quarantäneordnern auf den Geräten gespeichert wurden
- Dateien, die auf Client-Geräten in Backups verschoben wurden
- Dateien, für die Sicherheitsanwendungen eine verschobene Untersuchung festgelegt haben

Liste mit Objekten, die sich in der Datenverwaltung befinden, in eine Textdatei exportieren

Sie können alle Objekte, die sich der Datenverwaltung befinden, in eine Textdatei exportieren.

Um die Objektliste der Datenverwaltung in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum aus dem Ordner **Datenverwaltung** den Unterordner der gewünschten Datenverwaltung.

2. Wählen Sie im Unterordner der Datenverwaltung im Kontextmenü den Punkt **Liste exportieren** aus.

   Daraufhin öffnet sich das Fenster **Liste exportieren**, in dem Sie den Namen der Textdatei und den Ordnerpfad angeben können.

Installationspakete

Kaspersky Security Center legt Installationspakete für Kaspersky-Anwendungen und Drittanbieter-Anwendungen in der Datenverwaltung ab.

Das *Installationspaket* besteht aus mehreren Dateien, die für die Installation des Programms erforderlich sind. Das Installationspaket enthält Einstellungen zum Installationsvorgang und zur Erstkonfiguration des Programms.

Wenn Sie ein Programm auf einem Client-Gerät installieren möchten, müssen Sie für dieses Programm ein Installationspaket erstellen oder ein bereits erstelltes Installationspaket verwenden. Die Liste aller erstellten Installationspakete befindet sich im Konsolenbaum im Ordner **Remote-Installation** im Unterordner **Installationspakete**.

Grundlegende Statusvarianten der Dateien in der Datenverwaltung

Die Sicherheitsanwendungen untersuchen die Dateien auf den Geräten auf das Vorhandensein bekannter Viren und anderer Programme, die eine Bedrohung darstellen, weisen den Dateien einen Status zu und verschieben einige Dateien in die Datenverwaltung.

Sicherheitsanwendungen können z. B.

- eine Kopie der Datei vor ihrem Löschen in der Datenverwaltung speichern
- möglicherweise infizierte Dateien in der Datenverwaltung isolieren

Die grundlegenden Statusvarianten der Dateien finden Sie in der nachfolgenden Tabelle. Ausführliche Informationen über die Aktionen mit Dateien finden Sie in der Hilfe der Sicherheitsanwendungen.

Statusvarianten der Dateien in der Datenverwaltung

Name Status	Statusbeschreibung
Infiziert	In der Datei wurde das Code-Fragment eines bekannten Virus oder einer anderen Schadsoftware gefunden, das eine Bedrohung darstellt und über welches die Antiviren-Datenbanken von Kaspersky Informationen enthalten.
Virusfrei	In der Datei wurden weder ein bekannter Virus noch eine andere Schadsoftware gefunden.
Warnung	Die Datei enthält ein Code-Fragment, der teilweise mit dem Kontrollfragment des Codes einer bekannten Bedrohung übereinstimmt.
Möglicherweise infiziert	Die Datei enthält entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus ähnelt, der Kaspersky bisher nicht bekannt ist.
Vom Benutzer in den Ordner verschoben	Der Benutzer hat die Datei selbstständig in die Datenverwaltung verschoben, da das Verhalten der Datei z. B. den Verdacht erweckte, sie könnte eine Bedrohung enthalten. Der Benutzer kann die Datei mithilfe von aktualisierten Datenbanken auf das Vorhandensein von Bedrohungen untersuchen.
Fehlalarm	Die Kaspersky-Anwendung hat einer nicht infizierten Daten den Status "infiziert" zugewiesen, da ihr Code dem Code eines Virus ähnelt. Sie wird nach der Untersuchung mithilfe von aktualisierten Datenbanken als nicht infiziert eingestuft.
Desinfiziert	Die Datei konnte desinfiziert werden.
Gelöscht	Die Datei wurde infolge ihrer Verarbeitung gelöscht.
Mit Kennwort geschützt	Die Datei kann nicht verarbeitet werden, da sie kennwortgeschützt ist.

Auslösen von Regeln im Smart Training-Modus

Dieser Abschnitt enthält Informationen über die Funde, die mithilfe von Regeln der Adaptiven Kontrolle von Anomalien in Kaspersky Endpoint Security für Windows auf Client-Geräten erfolgt sind.

Die Regeln finden abnormales Verhalten auf Client-Geräten und können dieses blockieren. Wenn die Regeln im Smart Training-Modus ausgeführt werden, erkennen sie abnormales Verhalten und senden Berichte über jeden Fund an den Kaspersky Security Center Administrationsserver. Diese Informationen werden als Liste im Unterordner **Auslöser der Regel im Smart-Training-Status** des Ordners **Datenverwaltung** gespeichert. Sie können Funde als korrekt bestätigen oder sie den Ausnahmen hinzufügen, damit solches Verhalten in Zukunft nicht mehr als ungewöhnlich registriert wird.

Informationen über Funde werden im Ereignisprotokoll auf dem Administrationsserver (gemeinsam mit anderen Ereignissen) und im Bericht über die Adaptive Kontrolle von Anomalien gespeichert.

Weitere Informationen über die Regeln für die Adaptive Kontrolle von Anomalien, deren Modi und Statusvarianten finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Anzeigen der Liste der Funde mithilfe der Regeln für die Adaptive Kontrolle von Anomalien

So zeigen Sie die Liste der Funde an, die auf Regeln der Adaptiven Kontrolle von Anomalien beruhen:

1. Wählen Sie in der Konsolenstruktur den Knoten des erforderlichen Administrationsservers aus.
2. Wählen Sie den Unterordner **Auslöser der Regel im Smart-Training-Status** aus (standardmäßig ist dies ein Unterordner von **Erweitert** → **Datenverwaltung**).

   Die Liste enthält die folgenden Informationen zu den Funden, die auf Regeln der Adaptiven Kontrolle von Anomalien beruhen:

   - **Administrationsgruppe**

     Name der Administrationsgruppe, zu der das Gerät gehört.

   - **Gerätename**

     Name des Client-Geräts, auf das die Regel angewendet wurde.

   - **Name**

     Name der Regel, die angewendet wurde.

   - **Status**

     Excluding – Wenn der Administrator dieses Element verarbeitet und als Ausnahme für die Regeln hinzugefügt hat. Dieser Status bleibt bis zur nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver bestehen; nach der Synchronisierung wird das Element aus der Liste entfernt.

     Confirming – Wenn der Administrator dieses Element verarbeitet und bestätigt hat. Dieser Status bleibt bis zur nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver bestehen; nach der Synchronisierung wird das Element aus der Liste entfernt.

     Leer – Wenn der Administrator dieses Element nicht verarbeitet hat.

- **Anzahl der Regelauslösungen**

  Anzahl der Funde für eine heuristische Regel, einen Prozess und ein Client-Gerät. Diese Anzahl wird von Kaspersky Endpoint Security berechnet.

- **Benutzername**

  Name des Benutzers des Client-Geräts, der den Prozess ausgeführt hat, welcher den Fund erzeugt hat.

- **Pfad des Quellprozesses**

  Pfad des Quellprozesses, d. h. des Prozesses, der die Aktion durchführt (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Quellprozesses**

  SHA256-Hash der Datei des Quellprozesses (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Pfad des Quellobjekts**

  Pfad des Objekts, das den Prozess, gestartet hat (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Quellobjekts**

  SHA256-Hash der Quelldatei (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Pfad des Zielprozesses**

  Pfad des Zielprozesses (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Zielprozesses**

  SHA256-Hash der Zieldatei (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Pfad des Zielobjekts**

  Pfad des Zielobjekts (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Zielobjekts**

  SHA256-Hash der Zieldatei (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Bearbeitet**

  Datum, an dem die Anomalie gefunden wurde.

So zeigen Sie die Eigenschaften der einzelnen Informationselemente an:

1. Wählen Sie in der Konsolenstruktur den Knoten des erforderlichen Administrationsservers aus.
2. Wählen Sie den Unterordner **Auslöser der Regel im Smart-Training-Status** aus (standardmäßig ist dies ein Unterordner von **Erweitert** → **Datenverwaltung**).
3. Wählen Sie im Arbeitsbereich **Auslöser der Regel im Smart-Training-Status** das gewünschte Objekt aus.

4. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Informationsfeld auf der rechten Bildschirmseite auf den Link **Eigenschaften**.
   - Drücken Sie die rechte Maustaste und wählen Sie im Kontextmenü **Eigenschaften** aus.

   Das Eigenschaftenfenster des Objekts wird geöffnet und zeigt Informationen über das ausgewählte Element an.

Sie können ein beliebiges Element aus der Liste mit Funden der Regeln zur Adaptiven Kontrolle von Anomalien bestätigen oder zu den Ausnahmen hinzufügen.

So bestätigen Sie ein Element:

Klicken Sie auf ein Element (oder mehrere Elemente) in der Liste der Funde und anschließend auf **Bestätigen**.

Der Status des Elements bzw. der Elemente ändert sich in **Bestätigung**.

Ihre Bestätigung trägt zu der Statistik bei, die von den Regeln verwendet werden (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security 11 für Windows).

So fügen Sie ein Element zu den Ausnahmen hinzu:

Klicken Sie mit der rechten Maustaste auf ein Element (oder mehrere Elemente) in der Liste der Funde und wählen Sie im Kontextmenü **Zu Ausschlüssen hinzufügen** aus.

Der Assistent zum Hinzufügen von Ausnahmen wird gestartet. Folgen Sie den Anweisungen des Assistenten.

Wenn Sie ein Element ablehnen oder bestätigen, wird es nach der nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver aus der Liste der Funde ausgeschlossen und mehr in der Liste angezeigt.

Ausschlüsse aus den Regeln zur Adaptiven Kontrolle von Anomalien hinzufügen

Mit dem Assistenten zum Hinzufügen von Ausnahmen können Sie Ausnahmen für Regeln der Adaptiven Kontrolle von Anomalien in Kaspersky Endpoint Security hinzufügen.

Sie können den Assistenten durch eine der folgenden drei Prozeduren starten.

So starten Sie den Assistenten zum Hinzufügen von Ausnahmen über den Knoten "Adaptive Kontrolle von Anomalien":

1. Wählen Sie in der Konsolenstruktur den Knoten des gewünschten Administrationsservers aus.
2. Wählen Sie **Auslöser der Regel im Smart-Training-Status** (standardmäßig ist dies ein Unterordner von **Erweitert → Datenverwaltung**).
3. Klicken Sie im Arbeitsbereich mit der rechten Maustaste auf ein Element (oder mehrere Elemente) in der Liste der Funde und wählen Sie **Zu Ausschlüssen hinzufügen**.

   Sie können bis zu 1.000 Ausnahmen auf einmal hinzufügen. Wenn Sie mehr Elemente auswählen und versuchen, diese den Ausnahmen hinzuzufügen, erscheint eine Fehlermeldung.

   Daraufhin wird der Assistent für das Hinzufügen eines Ausschlusses gestartet.

Der Assistent für das Hinzufügen eines Ausschlusses kann aus anderen Knoten der Konsolenstruktur gestartet werden:

- Registerkarte **Ereignisse** im Hauptfenster des Administrationsservers (Option **Benutzeranfragen** oder **Letzte Ereignisse**).

- Spalte **Bericht zum Regelstatus der Adaptiven Kontrolle von Anomalien**, **Anzahl der Funde**.

Schritt 1. Auswählen des Programms

Dieser Schritt kann übersprungen werden, wenn Sie nur über ein Kaspersky Endpoint Security für Windows verfügen und keine anderen Anwendungen haben, welche die Regeln für die Adaptive Kontrolle von Anomalien verwenden.

Der Assistent für das Hinzufügen eines Ausschlusses zeigt eine Liste mit Kaspersky-Anwendungen an, deren Verwaltungs-Plug-ins das Hinzufügen von Ausschlüssen zu den Richtlinien dieser Programme erlauben. Wählen Sie ein Programm in der Liste aus und klicken Sie auf **Weiter**, um zur Auswahl der Richtlinie zu gelangen, zu welcher der Ausschluss hinzugefügt wird.

Schritt 2. Auswählen der Richtlinie (Richtlinien)

Der Assistent zeigt die Liste der Richtlinien (mit Richtlinienprofilen) für Kaspersky Endpoint Security an.

Wählen Sie alle Richtlinien und Profile aus, zu denen Sie Ausschlüsse hinzufügen möchten, und klicken Sie auf **Weiter**.

Schritt 3. Verarbeiten der Richtlinie (Richtlinien)

Der Assistent zeigt einen Fortschrittsbalken an, während die Richtlinien verarbeitet werden. Sie können die Verarbeitung von Richtlinien unterbrechen, indem Sie auf **Abbrechen** klicken.

Geerbte Richtlinien können nicht aktualisiert werden. Wenn Sie keine Berechtigungen zum Ändern einer Richtlinie haben, wird diese Richtlinie ebenfalls nicht aktualisiert.

Sobald alle Richtlinien verarbeitet wurden (oder wenn Sie die Verarbeitung abbrechen), wird ein Bericht angezeigt. Dieser zeigt, welche Richtlinien erfolgreich aktualisiert wurden (grünes Symbol) und welche Richtlinien nicht aktualisiert wurden (rotes Symbol).

Dies ist der letzte Schritt des Assistenten. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

Quarantäne und Backup

Auf den Client-Geräten installierte Antiviren-Programme von Kaspersky können während der Untersuchung von Geräten die Dateien in Quarantäne oder ins Backup verschieben.

Die *Quarantäne* ist ein spezieller Speicher, in den Dateien verschoben werden, die möglicherweise von Viren infiziert oder im Augenblick des Fundes irreparabel sind.

Das *Backup* dient zur Speicherung der Backup-Kopien von Dateien, die gelöscht oder bei der Desinfizierung verändert wurden.

Kaspersky Security Center erstellt eine gemeinsame Liste von Dateien, die von Kaspersky-Anwendungen auf den Client-Geräten in die Quarantäne oder ins Backup verschoben werden. Die Administrationsagenten der Client-Geräte leiten Informationen über die Dateien in der Quarantäne und im Backup an den Administrationsserver weiter. Über die Verwaltungskonsole können Sie die Eigenschaften der Dateien in der Datenverwaltung der Geräte ansehen, die Untersuchung der Datenverwaltung auf Schadsoftware starten und Dateien aus der Datenverwaltung löschen. Die Symbole der Statusvarianten der Dateien werden im Anhang beschrieben.

Die Vorgänge mit Quarantäne und Backup werden für Kaspersky Endpoint Security unterstützt.

Kaspersky Security Center kopiert keine Dateien aus der Datenverwaltung auf den Administrationsserver. Alle Dateien werden in der Datenverwaltung auf den Geräten abgelegt. Die Wiederherstellung der Dateien auf dem Gerät kann nur mit der Antiviren-Anwendung erfolgen, welche die Datei in die Datenverwaltung verschoben hat.

Aktivieren der Remote-Verwaltung von Dateien in der Datenverwaltung

Standardmäßig ist die Remote-Verwaltung von Dateien in der Datenverwaltung auf den Client-Geräten deaktiviert.

Um die Remote-Verwaltung von Dateien in der Datenverwaltung auf den Client-Geräten zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum die Administrationsgruppe, für welche die Remote-Verwaltung der Dateien aktiviert werden soll.
2. Öffnen Sie im Arbeitsbereich der Gruppe die Registerkarte **Richtlinien**.
3. Wählen Sie unter **Richtlinien** die Richtlinie der Sicherheitsanwendung, welche die Dateien auf den Geräten in die Datenverwaltung verschiebt.
4. Aktivieren Sie im Fenster der Richtlinieneigenschaften im Einstellungsblock **Datenübertragung an den Administrationsserver** die Kontrollkästchen jeder Datenverwaltungsart, für die Sie die Remote-Verwaltung aktivieren möchten.

   Die Lage der Einstellungsgruppe **Datenübertragung an den Administrationsserver** im Fenster der Richtlinieneigenschaften sowie die Beschriftungen der Kontrollkästchen sind spezifisch für jede Sicherheitsanwendung.

Eigenschaften der Datei in der Datenverwaltung anzeigen

Um Eigenschaften einer Datei in Quarantäne oder im Backup anzusehen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Quarantäne** oder **Backup**.
2. Im Arbeitsbereich des Ordners **Quarantäne** (**Backup**) wählen Sie die Datei aus, deren Eigenschaften angezeigt werden sollen.
3. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Eigenschaften** aus.

Dateien aus der Datenverwaltung entfernen

Um eine Datei in Quarantäne oder im Backup zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Datenverwaltung** entweder den Unterordner **Quarantäne** oder **Backup**.
2. Wählen Sie im Arbeitsbereich des Ordners **Quarantäne** (oder **Backup**) die zu löschenden Dateien aus. Verwenden Sie dazu die Tasten **Umschalt** und **Strg**.
3. Löschen Sie die Dateien auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf die Dateien und wählen Sie **Entfernen** aus.
   - Klicken Sie auf den Link **Löschen** (**Löschen**, falls nur eine Datei gelöscht werden soll) im Informationsfeld für die Bearbeitung der ausgewählten Dateien.

Daraufhin werden diese Dateien, die von den Sicherheitsanwendungen in die Datenverwaltung der Client-Geräte verschoben wurden, aus der jeweiligen Datenverwaltung gelöscht.

Dateien aus der Datenverwaltung wiederherstellen

Um eine Datei aus der Quarantäne oder aus dem Backup wiederherzustellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Quarantäne** oder **Backup**.
2. Wählen Sie im Arbeitsbereich des Ordners **Quarantäne** (**Backup**) Dateien aus, die wiederhergestellt werden sollen. Verwenden Sie dazu die Tasten **Umschalt** und **Strg**.
3. Starten Sie den Wiederherstellungsprozess der Dateien auf eine der folgenden Arten:
   - Klicken Sie mit der rechten Maustaste auf die betreffenden Dateien und wählen Sie **Wiederherstellen** aus.
   - Klicken Sie auf den Link **Wiederherstellen** im Informationsfeld der ausgewählten Dateien.

Daraufhin werden diese Dateien, die von den Sicherheitsanwendungen in die Datenverwaltung der Client-Geräte verschoben wurden, in den ursprünglichen Ordnern wiederhergestellt.

Datei aus der Datenverwaltung auf der Festplatte speichern

Kaspersky Security Center ermöglicht es, Kopien der Dateien auf dem Laufwerk zu speichern, die von den Sicherheitsanwendungen in die Quarantäne oder ins Backup des Client-Geräts verschoben wurden. Die Dateien werden auf das Gerät mit Kaspersky Security Center in den von Ihnen angegebenen Ordner kopiert.

Um eine Kopie der Datei aus der Quarantäne oder dem Backup auf eine Festplatte zu speichern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Quarantäne** oder **Backup**.
2. Wählen Sie im Arbeitsbereich des Ordners **Quarantäne** (**Backup**) eine Datei aus, die auf die Festplatte kopiert werden soll.

3. Starten Sie den Kopiervorgang der Datei auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Auf Datenträger speichern** aus.
   - Klicken Sie auf den Link **Auf Datenträger speichern** im Informationsfeld der ausgewählten Datei.

Die Sicherheitsanwendung, welche die Datei in die Quarantäne auf dem Client-Gerät verschoben hat, speichert eine Kopie der Datei in dem vom Administrator angegebenen Ordner.

Untersuchung der Dateien in Quarantäne

Um Dateien zu untersuchen, die sich in Quarantäne befinden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Quarantäne** aus.
2. Im Arbeitsbereich des Ordners **Quarantäne** wählen Sie mithilfe der Tasten **`Umschalt`** und **`Strg`** die Dateien, die untersucht werden sollen.
3. Starten Sie die Untersuchung für Dateien auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Untersuchen** aus.
   - Klicken Sie im Informationsfeld mit den ausgewählten Dateien auf den Link **Untersuchen**.

   Daraufhin wird für die Sicherheitsanwendungen, die Dateien in Quarantäne verschoben haben, eine Aufgabe zur Untersuchung auf Befehl auf den Client-Geräten gestartet, auf denen sich die in Quarantäne verschobenen Dateien befinden.

Aktive Bedrohungen

Informationen über unverarbeitete Dateien, die sich auf den Client-Geräten befinden, finden Sie im Ordner **Datenverwaltung** im Unterordner **Aktive Bedrohungen**.

Die verschobene Verarbeitung und die Desinfektion von Dateien mithilfe der Sicherheitsanwendung werden auf Befehl oder nach Eintreten eines bestimmten Ereignisses ausgeführt. Sie können Einstellungen der verschobenen Desinfektion von Dateien anpassen.

Unverarbeitete Dateien desinfizieren

Um die Desinfektion einer unverarbeiteten Datei zu starten, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Aktive Bedrohungen** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Aktive Bedrohungen** die Datei aus, die desinfiziert werden soll.

3. Starten Sie den Vorgang der Desinfektion der Datei auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Desinfizieren** aus.
   - Klicken Sie auf den Link **Desinfizieren** im Informationsfeld der ausgewählten Datei.

   Es wird daraufhin versucht, die Datei zu desinfizieren:

Wenn die Datei desinfiziert wurde, stellt die auf dem Client-Gerät installierte Sicherheitsanwendung die Datei im ursprünglichen Ordner wieder her. Der Eintrag für diese Datei wird aus der Liste im Ordner **Aktive Bedrohungen** gelöscht. Wenn eine Desinfektion der Datei nicht möglich ist, löscht die auf dem Gerät installierte Sicherheitsanwendung die Datei vom Gerät. Der Eintrag für diese Datei wird aus der Liste im Ordner **Aktive Bedrohungen** gelöscht.

Die Möglichkeiten zur Desinfektion und Löschung von Dateien können je nach installierter Sicherheitsanwendung, Version und Einstellungen variieren.

Datei mit verschobener Verarbeitung auf Festplatte speichern

Kaspersky Security Center ermöglicht Ihnen das Speichern von Kopien unverarbeiteter Dateien, die auf den Client-Geräten gefunden wurden. Dies bezieht sich auf Dateien, die von der Anwendung desinfiziert oder gelöscht wurden. Die Dateien werden auf das Gerät mit Kaspersky Security Center in den von Ihnen angegebenen Ordner kopiert.

Sie können Kopien von Dateien speichern, wenn Dateien im Zuge ihre Desinfektion gelöscht oder verändert wurden. Die Kopien dieser Dateien werden auf dem verwalteten Gerät im Speicher von Kaspersky Endpoint Security für Windows abgelegt.

Um eine Kopie der Datei mit verschobener Verarbeitung auf der Festplatte zu speichern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Aktive Bedrohungen** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Aktive Bedrohungen** die Dateien aus, die auf die Festplatte kopiert werden sollen.
3. Starten Sie den Kopiervorgang der Datei auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Auf Datenträger speichern** aus.
   - Klicken Sie auf den Link **Auf Datenträger speichern** im Informationsfeld der ausgewählten Datei.

Daraufhin speichert die Sicherheitsanwendung des Client-Geräts, auf dem die ausgewählte unverarbeitete Datei gefunden wurde, eine Kopie der Datei im angegebenen Ordner.

Datei aus dem Ordner "Aktive Bedrohungen" löschen

*Um eine Datei aus dem Ordner **Aktive Bedrohungen** zu löschen:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Aktive Bedrohungen** aus.
2. Wählen Sie im Arbeitsbereich des Ordners **Aktive Bedrohungen** die zu löschenden Dateien aus. Verwenden Sie dazu die Tasten **Umschalt** und **Strg**.

3. Löschen Sie die Dateien auf eine der folgenden Arten:

   - Klicken Sie mit der rechten Maustaste auf die Dateien und wählen Sie **Entfernen** aus.
   - Klicken Sie auf den Link **Löschen** (**Löschen**, falls nur eine Datei gelöscht werden soll) im Informationsfeld für die Bearbeitung der ausgewählten Dateien.

Daraufhin werden diese Dateien, die von den Sicherheitsanwendungen in die Datenverwaltung der Client-Geräte verschoben wurden, aus der jeweiligen Datenverwaltung gelöscht. Die Einträge für diese Dateien werden aus der Liste im Ordner **Aktive Bedrohungen** gelöscht.

Kaspersky Security Network (KSN)

In diesem Abschnitt wird die Verwendung der Infrastruktur der Online-Dienste von Kaspersky Security Network (KSN) beschrieben. Er enthält Informationen über KSN sowie Anleitungen zur Aktivierung von KSN, zur Konfiguration des Zugriffs auf KSN und über die Statistiken der Verwendung des KSN-Proxyservers.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Über KSN

Das Kaspersky Security Network (KSN) ist eine Infrastruktur von Online-Diensten, die Zugriff auf die aktuelle Wissensdatenbank von Kaspersky bietet, in der Informationen über die Reputation der Dateien, Web-Ressourcen und Programme enthalten sind. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. Mit KSN können aus den Kaspersky-Reputations-Datenbanken Informationen über die Anwendungen abgerufen werden, die auf den verwalteten Geräten installiert sind.

Kaspersky Security Center unterstützt die folgenden Infrastrukturlösungen:

- *KSN* ist eine Lösung, mit der Sie Informationen mit dem Kaspersky Security Network austauschen können. Wenn Sie an KSN teilnehmen, stimmen Sie zu, dass Informationen über die Ausführung der auf den Client-Geräten installierten Kaspersky-Anwendungen, die von Kaspersky Security Center verwaltet werden, automatisch an Kaspersky übertragen werden. Die Übertragung von Informationen erfolgt gemäß den aktuellen Einstellungen für den Zugriff auf KSN. Kaspersky-Analysten analysieren zusätzlich erhaltene Informationen und nehmen sie in die Reputations- und Statistikdatenbanken von Kaspersky Security Network auf. Kaspersky Security Center verwendet standardmäßig diese Lösung.
- *Kaspersky Private Security Network (KPSN)* ist eine Lösung, die es Benutzern von Geräten mit installierten Kaspersky-Anwendungen ermöglicht, Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network und andere statistische Daten zu erhalten, ohne Daten von ihren eigenen Geräten an Global KSN zu senden. KPSN richtet sich an Unternehmenskunden, die aus einem der folgenden Gründe nicht an Kaspersky Security Network teilnehmen können:
  - Die Benutzergeräte haben keine Internetverbindung.
  - Die Übermittlung von Daten an einen Punkt außerhalb des Landes oder außerhalb des lokalen Unternehmensnetzwerks ist gesetzlich oder aufgrund von Sicherheitsrichtlinien des Unternehmens untersagt.

Sie können die Zugriffseinstellungen von Kaspersky Private Security Network im Abschnitt **KSN Proxy-Einstellungen** des Eigenschaftenfensters des Administrationsservers einstellen.

Die Programm fordert Sie auf, während der Ausführung des Schnellstartassistenten eine Verbindung zu KSN herzustellen. Sie können während der Ausführung des Programms jederzeit mit der Verwendung von KSN beginnen oder auf KSN verzichten.

Sie verwenden KSN gemäß der KSN-Erklärung, die Sie lesen und akzeptieren, wenn Sie KSN aktivieren. Wird die KSN-Erklärung aktualisiert, so wird sie Ihnen bei einem Upgrade der Version des Administrationsservers angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, verwenden Sie KSN weiterhin gemäß der vorherigen Version der KSN-Erklärung, die Sie zuvor akzeptiert haben.

Wenn KSN aktiviert ist, prüft Kaspersky Security Center, ob auf die KSN-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Dies ist notwendig, um sicherzustellen, dass das Sicherheitsniveau für die verwalteten Geräte beibehalten wird.

Vom Administrationsserver verwaltete Client-Geräte interagieren mithilfe des KSN-Proxyservers mit KSN. Der KSN-Proxyserver bietet folgende Möglichkeiten:

- Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen.
- Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Die Einstellungen des KSN-Proxyservers können Sie im Abschnitt **KSN Proxy-Einstellungen** im Eigenschaftenfenster des Administrationsservers ändern.

Zugriff auf Kaspersky Security Network vorbereiten

Sie können den Zugriff auf Kaspersky Security Network (KSN) auf dem Administrationsserver und auf einem Verteilungspunkt anpassen.

Um den Zugriff des Administrationsservers auf Kaspersky Security Network (KSN) einzurichten, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den der Zugriff auf KSN angepasst werden soll.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Fenster "Eigenschaften des Administrationsservers" im Bereich **Abschnitte** die Option **KSN Proxy → KSN Proxy-Einstellungen** aus.
4. Aktivieren Sie im Arbeitsbereich die Option **Administrationsserver als Proxyserver verwenden**, um den KSN-Proxy-Service zu aktivieren.

   Die Übertragung von Daten der Client-Geräte an KSN wird durch die Richtlinie von Kaspersky Endpoint Security geregelt, die auf den Client-Geräten in Kraft ist. Wenn das Kontrollkästchen deaktiviert ist, findet keine Übertragung von Daten des Administrationsservers bzw. der Client-Geräte über Kaspersky Security Center an KSN statt. In diesem Fall können die Client-Geräte Daten entsprechend ihrer Einstellungen direkt an KSN übertragen (nicht über Kaspersky Security Center). Die auf den Client-Geräten geltende Richtlinie für Kaspersky Endpoint Security für Windows bestimmt, welche Daten diese Geräte direkt (nicht über Kaspersky Security Center) an KSN senden.

5. Aktivieren Sie die Option **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**.

   Wenn diese Option aktiviert ist, senden Client-Geräte die Ergebnisse der Patch-Installation an Kaspersky. Wenn Sie diese Option aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.

   Wenn Sie das Kaspersky Private Security Network verwenden, aktivieren Sie die Option **KPSN konfigurieren** und klicken Sie auf **Datei mit KSN Proxy-Einstellungen wählen**, um die Einstellungen für KPSN herunterzuladen (Dateien mit den Erweiterungen pkcs7 und pem). Nach dem Herunterladen der Einstellungen werden in der Benutzeroberfläche die Bezeichnung des Providers, die Kontaktdaten des Providers und das Erstellungsdatum der Datei mit KPSN-Einstellungen angezeigt.

   > Wenn Sie KPSN aktivieren, achten Sie auf die Verteilungspunkte, die so konfiguriert wurden, dass sie KSN-Anfragen direkt an Cloud-KSN versenden. Verteilungspunkte mit installiertem Administrationsagent Version 11 (oder früher) senden weiterhin KSN-Anfragen an Cloud-KSN. Um die Verteilungspunkte so anzupassen, dass KSN-Anfragen an KPSN gesendet werden, aktivieren Sie für jeden Verteilungspunkt die Option **KSN-Anfragen an den Administrationsserver weiterleiten**. Sie können diese Option in den Eigenschaften des Verteilungspunkts oder in der Richtlinie des Administrationsagenten aktivieren.

   Wenn Sie das Kontrollkästchen **KPSN konfigurieren** aktivieren, erscheint eine Meldung mit den Details zu KPSN.

   Wenn Sie in Kaspersky Security Center die Option **KPSN konfigurieren** aktivieren, erhalten diese Anwendungen Informationen über die Unterstützung von KPSN. Im Unterabschnitt **Kaspersky Security Network** des Abschnitts **Erweiterter Schutz** wird im Fenster "Einstellungen" die Information zum ausgewählten KSN-Anbieter angezeigt: Entweder KSN oder KPSN.

   > Wenn Sie für die Arbeit mit KPSN ältere Programmversionen als Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 oder Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent verwenden, ist es empfehlenswert, die sekundären Administrationsserver zu verwenden, für welche die Nutzung von KPSN nicht konfiguriert ist.

   > Kaspersky Security Center sendet keine statistischen Daten an Kaspersky Security Network, wenn KPSN im Abschnitt **KSN Proxy → KSN Proxy-Einstellungen** des Fensters "Eigenschaften des Administrationsservers" angepasst ist.

   Wenn Sie die Proxyserver-Einstellungen in den Eigenschaften des Administrationsservers angepasst haben, aber Ihre Netzwerkarchitektur eine direkte Verwendung von KPSN erfordert, aktivieren Sie die Option **Proxyserver-Einstellungen beim Verbinden mit KPSN ignorieren**. Andernfalls können Anfragen von den verwalteten Apps KPSN nicht erreichen.

6. Passen Sie die Einstellungen für die Verbindung des Administrationsservers mit dem Dienst des KSN-Proxy-Service an:

   - Geben Sie unter **Verbindungseinstellungen** für den **TCP-Port** die Nummer des TCP-Ports an, über den die Verbindung zum KSN-Proxyserver aufgebaut werden soll. Standardmäßig erfolgt die Verbindung zum KSN-Proxyserver über Port 13111.

   - Wenn Sie möchten, dass der Administrationsserver die Verbindung zum KSN-Proxyserver über einen UDP-Port herstellt, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine Portnummer für den **UDP-Port** an. Standardmäßig ist diese Option deaktiviert und der TCP-Port wird verwendet. Wenn diese Option aktiviert wird, ist 15111 der standardmäßige UDP-Port für die Verbindung mit dem KSN-Proxyserver.

   - Wenn die verwalteten Geräte eine Verbindung mit dem Administrationsserver über einen HTTPS-Port herstellen sollen, aktivieren Sie die Option **HTTPS über Port** und geben Sie anschließend eine Portnummer an. Standardmäßig ist diese Option deaktiviert und der TCP-Port wird verwendet. Wenn diese Option aktiviert wird, ist 17111 der standardmäßige HTTPS-Port für die Verbindung mit dem KSN-Proxyserver.

7. Aktivieren Sie die Option **Sekundäre Administrationsserver über den primären Administrationsserver mit KSN verbinden**.

   Wenn diese Option aktiviert ist, verwenden die sekundären Administrationsserver jeder Hierarchieebene den primären Administrationsserver als KSN-Proxyserver. Wenn diese Option deaktiviert ist, verbinden sich die sekundären Administrationsserver selbständig mit KSN. In diesem Fall verwenden die verwalteten Geräte die sekundären Administrationsserver als KSN-Proxyserver.

   > Die sekundären Administrationsserver verwenden den primären Administrationsserver als Proxyserver, wenn in den Eigenschaften der sekundären Administrationsserver im rechten Bereich im Abschnitt **KSN Proxy-Einstellungen** das Kontrollkästchen **Administrationsserver als Proxyserver verwenden** aktiviert ist.

8. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin werden die Einstellungen für den Zugriff auf KSN gespeichert.

Sie können außerdem den Zugriff des Verteilungspunkts auf KSN anpassen, um z. B. die Auslastung des Administrationsservers zu reduzieren. Der Verteilungspunkt, der als KSN-Proxyserver fungiert, sendet KSN-Anfragen von verwalteten Geräten direkt an Kaspersky, ohne den Administrationsserver zu verwenden.

Um den Zugriff des Verteilungspunkts auf Kaspersky Security Network (KSN) einzurichten, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Verteilungspunkt manuell zugewiesen wurde.
2. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
3. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
4. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Verteilungspunkte** aus.
5. Wählen Sie den Verteilungspunkt in der Liste aus und öffnen Sie mithilfe der Schaltfläche **Eigenschaften** das entsprechende Eigenschaftenfenster.

6. Wählen Sie im Eigenschaftenfenster des Verteilungspunkts im Abschnitt **KSN-Proxy** den Punkt **Direkt über das Internet auf KSN Cloud/KPSN zugreifen** aus.

7. Klicken Sie auf die Schaltfläche **OK**.

Der Verteilungspunkt wird nun als KSN-Proxyserver fungieren.

KSN aktivieren und deaktivieren

Um KSN zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den KSN aktiviert werden soll.

2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN Proxy** den Unterabschnitt **KSN Proxy-Einstellungen**.

4. Wählen Sie **Administrationsserver als Proxyserver verwenden**.

   Der Dienst des KSN-Proxyservers wird aktiviert.

5. Aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**.

   Daraufhin wird KSN aktiviert.

   Wenn dieses Kontrollkästchen aktiviert ist, werden die Ergebnisse der Installation von Patches von den Client-Geräten an Kaspersky übermittelt. Wenn Sie das Kontrollkästchen aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.

6. Klicken Sie auf die Schaltfläche **OK**.

Um die KSN zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den KSN aktiviert werden soll.

2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN Proxy** den Unterabschnitt **KSN Proxy-Einstellungen**.

4. Deaktivieren Sie das Kontrollkästchen **Administrationsserver als Proxyserver verwenden**, um den KSN-Proxy-Service zu deaktivieren, oder deaktivieren Sie das Kontrollkästchen **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**.

   Ist das Kontrollkästchen deaktiviert, werden von den Client-Geräten keine Ergebnisse der Installation von Patches an Kaspersky übermittelt.

   Wenn Sie KPSN verwenden, deaktivieren Sie das Kontrollkästchen **KPSN konfigurieren**.

   Daraufhin wird KSN deaktiviert.

5. Klicken Sie auf die Schaltfläche **OK**.

Die akzeptierte KSN-Erklärung anzeigen

Wenn Sie Kaspersky Security Network (KSN) aktivieren, müssen Sie die KSN-Erklärung lesen und akzeptieren. Sie können die akzeptierte KSN-Erklärung jederzeit anzeigen.

So zeigen Sie die akzeptierte KSN-Erklärung an:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den Sie KSN aktiviert haben.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN Proxy** den Unterabschnitt **KSN Proxy-Einstellungen**.
4. Klicken Sie auf den Link **Akzeptierte KSN-Erklärung anzeigen**.

   Im folgenden Fenster können Sie den Text der akzeptierten KSN-Erklärung anzeigen.

KSN-Proxyserver-Statistik anzeigen

Der *KSN-Proxyserver* ist ein Dienst, der die Interaktion zwischen der Infrastruktur Kaspersky Security Network und den Client-Geräten, die vom Administrationsserver verwaltet werden, gewährleistet.

Die Verwendung des KSN-Proxyservers bietet Ihnen folgende Möglichkeiten:

- Client-Geräte können Anfragen an KSN initiieren und an KSN Informationen übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen.
- Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Im Eigenschaftenfenster des Administrationsservers können Sie die Einstellungen des KSN-Proxyservers anpassen und statistische Daten über die Verwendung des KSN-Proxyservers anzeigen.

Um die KSN-Proxyserver-Statistiken anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den die KSN-Statistik angezeigt werden soll.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN Proxy** den Unterabschnitt **KSN Proxy-Statistik**.

   Dieser Abschnitt zeigt die aktuellen Ausführungsstatistiken des KSN-Proxyservers an (Anzahl der Datensätze im Cache, der verarbeitete Pakete im Cache und der empfangene Pakete). Wenn der Administrationsserver mit KSN verbunden ist, wird außerdem eine entsprechende Informationsmeldung angezeigt.

Führen Sie erforderlichenfalls zusätzliche Aktionen aus:

- Aktualisieren Sie mithilfe der Schaltfläche **Aktualisieren** die Statistikdaten über die Verwendung des KSN-Proxyservers.
- Exportieren Sie mithilfe der Schaltfläche **In Datei exportieren** Statistikdaten in eine csv-Datei.
- Überprüfen Sie mithilfe der Schaltfläche **KSN-Verbindung überprüfen**, ob der Administrationsserver derzeit mit KSN verbunden ist.

4. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Administrationsservers zu schließen.

Eine aktualisierte KSN-Erklärung akzeptieren

Sie verwenden KSN gemäß der KSN-Erklärung, die Sie lesen und akzeptieren, wenn Sie KSN aktivieren. Wird die KSN-Erklärung aktualisiert, so wird sie Ihnen bei einem Upgrade oder einer Aktualisierung des Administrationsservers angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, verwenden Sie KSN weiterhin gemäß der Version der KSN-Erklärung, die Sie zuvor akzeptiert haben.

Nach einem Update oder einem Upgrade des Administrationsservers wird die aktualisierte KSN-Erklärung automatisch angezeigt. Wenn Sie die aktualisierte KSN-Erklärung ablehnen, können Sie diese später erneut anzeigen und akzeptieren.

Um die KSN-Erklärung anzuzeigen und anschließend zu akzeptieren:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Klicken Sie auf der Registerkarte **Überwachung** im Abschnitt **Überwachung** auf den Link **Die akzeptierte Erklärung zu Kaspersky Security Network ist veraltet**.

   Das Fenster mit der **KSN-Erklärung** öffnet sich.
3. Lesen Sie sich die KSN-Erklärung sorgfältig durch und treffen Sie anschließend eine Entscheidung. Wenn Sie die aktualisierte KSN-Erklärung akzeptieren, klicken Sie auf die Schaltfläche **Ich akzeptiere die Bedingungen des Lizenzvertrags**. Wenn Sie die KSN-Erklärung ablehnen, klicken Sie auf die Schaltfläche **Abbrechen**.

Entsprechend Ihrer Entscheidung funktioniert KSN in Übereinstimmung mit den Bedingungen der aktuellen oder der aktualisierten KSN-Erklärung. Das Anzeigen des Textes der akzeptierten KSN-Erklärung ist jederzeit in den Eigenschaften des Administrationsservers möglich.

Zusätzlicher Schutz durch Verwendung von Kaspersky Security Network

Kaspersky bietet ein zusätzliches Schutzniveau durch die Verwendung von Kaspersky Security Network. Ziel dieser Schutzmethode ist der effektive Kampf gegen komplizierte, ständig auftauchende Bedrohungen, sowie Zero-Day-Bedrohungen. Die mit Kaspersky Endpoint Security integrierten Cloud-Technologien und fachspezifische Kenntnisse der Virenanalysten von Kaspersky ermöglichen einen umfangreichen Schutz gegen die kompliziertesten Bedrohungen im Netzwerk.

Weitere Informationen über den zusätzlichen Schutz von Kaspersky Endpoint Security finden Sie auf der Kaspersky-Website.

Feststellen, ob der Verteilungspunkt als KSN-Proxyserver fungiert

Sie können auf einem verwalteten Gerät, welches als Verteilungspunkt fungiert, den KSN-Proxyserver aktiveren. Ein verwaltetes Gerät funktioniert als KSN-Proxyserver, wenn auf dem Gerät der Dienst "ksnproxy" ausgeführt wird. Sie können diesen Dienst lokal auf dem Gerät überprüfen, aktivieren und deaktivieren.

Sie können einem Windows-basierten oder Linux-basierten Gerät die Rolle des Verteilungspunkts zuweisen. Die Methode zur der Überprüfung des Verteilungspunkts hängt vom Betriebssystem dieses Verteilungspunkts ab.

So stellen Sie fest, ob der Windows-basierte Verteilungspunkt als KSN-Proxyserver fungiert:

1. Öffnen Sie auf dem Gerät mit dem Verteilungspunkt unter Windows die **Dienste**-App (**Alle Programme** → **Windows Verwaltungsprogramme** → **Dienste**).

2. Prüfen Sie in der Liste der Dienste, ob der Dienst ksnproxy ausgeführt wird.

   Wenn der Dienst "ksnproxy" ausgeführt wird, nimmt der Administrationsagent auf diesem Gerät an Kaspersky Security Network teil und fungiert als KSN-Proxyserver für verwaltete Geräte, die sich im Bereich des Verteilungspunkts befinden.

Bei Bedarf können Sie den Dienst ksnproxy deaktivieren. In diesem Fall nimmt der Administrationsagent des Verteilungspunkts nicht länger an Kaspersky Security Network teil. Dieser Vorgang erfordert lokale Administratorrechte.

So stellen Sie fest, ob der Linux-basierte Verteilungspunkt als KSN-Proxyserver fungiert:

1. Zeigen Sie auf dem Gerät, dass als Verteilungspunkt fungiert, die Liste der ausgeführten Prozesse an.

2. Überprüfen Sie, ob in der Liste der laufenden Prozesse, der Prozess `/[[/opt/kaspersky/ksc64/sbin/ksnproxy]]` ausgeführt wird.

Wenn der Dienst `/opt/kaspersky/ksc64/sbin/ksnproxy` ausgeführt wird, nimmt der Administrationsagent auf diesem Gerät an Kaspersky Security Network teil und fungiert als KSN-Proxyserver für verwaltete Geräte, die sich im Bereich des Verteilungspunkts befinden.

Zwischen Online-Hilfe und Offline-Hilfe wechseln

Wenn Sie keinen Zugang zum Internet haben, können Sie die Offline-Hilfe verwenden.

So wechseln Sie zwischen Online-Hilfe und Offline-Hilfe:

1. Wählen Sie im Hauptfenster von Kaspersky Security Center in der Konsolenstruktur den Punkt **Kaspersky Security Center 15.1** aus.

2. Klicken Sie auf den Link **Globale Einstellungen der Benutzeroberfläche**.

   Das Einstellungsfenster wird geöffnet.

3. Klicken Sie im Fenster auf **Offline-Hilfe verwenden**.

4. Klicken Sie auf die Schaltfläche **OK**.

Die Einstellungen werden übernommen und gespeichert. Sie können die Einstellungen jederzeit rückgängig machen und die Online-Hilfe verwenden.

Ereignisse in SIEM-Systeme exportieren

In diesem Abschnitt wird der Ablauf des Exports von Ereignissen, die in Kaspersky Security Center registriert sind, in externe Systeme zur Ereignisverwaltung der Informationssicherheit (SIEM-System, Security Information and Event Management) beschrieben.

Ereignisexport in SIEM-Systeme konfigurieren

Kaspersky Security Center ermöglicht die Konfiguration mit einer der folgenden Methoden: Export in ein beliebiges SIEM-System mit Syslog-Format; Export in die SIEM-Systeme QRadar, Splunk, ArcSight mit LEEF- und CEF-Format; direkter Export von Ereignissen in SIEM-Systeme aus der Datenbank von Kaspersky Security Center. Nach Abschluss dieses Szenarios sendet der Administrationsserver Ereignisse automatisch an das SIEM-System.

Erforderliche Vorrausetzungen

Bevor Sie mit der Konfiguration des Ereignisexports in die Kaspersky Security Center beginnen:

- Erfahren Sie mehr über die Exportmethoden.
- Stellen Sie sicher, dass Sie die Werte der Systemeinstellungen kennen.

Sie können die Schritte in diesem Szenario in beliebiger Reihenfolge ausführen.

Der Prozess des Ereignisexports in SIEM-Systeme umfasst die folgenden Schritte:

- **Konfigurieren des SIEM-Systems, so dass es Ereignisse aus Kaspersky Security Center empfängt**

  Anleitung: Einstellungen für den Ereignisexport in das SIEM-System

- **Auswählen der Ereignisse, die Sie in das SIEM-System exportieren möchten:**

  Anleitung:

  - Verwaltungskonsole: Ereignisse einer Kaspersky-Anwendung für den Export im Syslog-Format markieren, Allgemeine Ereignisse für den Export im Syslog-Format markieren
  - Kaspersky Security Center Web Console: Ereignisse einer Kaspersky-Anwendung für den Export im Syslog-Format markieren, Allgemeine Ereignisse für den Export im Syslog-Format markieren

- **Konfigurieren des Ereignisexports in ein SIEM-System unter Verwendung einer der folgenden Methoden:**

  - Mittels der Protokolle TCP, UDP oder TLS over TCP.

Anleitung:

- Verwaltungskonsole: Export von Ereignissen in SIEM-Systeme konfigurieren
- Kaspersky Security Center Web Console: Export von Ereignissen in SIEM-Systeme konfigurieren

- Mittels direktem Ereignisexport aus der Datenbank von Kaspersky Security Center (In der Datenbank von Kaspersky Security Center ist eine Auswahl an öffentlichen Ansichten verfügbar. Die Beschreibung dieser Ansichten finden Sie im Dokument klakdb.chm).

Ergebnisse

Nach der Konfiguration des Ereignisexports in ein SIEM-System, können Sie sich die Exportergebnisse ansehen, wenn Sie Ereignisse ausgewählt haben, die Sie exportieren wollen.

Vorläufige Bedingungen

Bei den Einstellungen für den automatischen Ereignisexport in Kaspersky Security Center müssen einige Einstellungen des SIEM-Systems angegeben werden. Es ist empfehlenswert, diese Einstellungen im Voraus zu bestimmen, damit die Einstellungen für Kaspersky Security Center vorbereitet werden können.

Für die Einstellungen des automatischen Ereignisexports ins SIEM-System müssen die Werte der folgenden Einstellungen bekannt sein:

- **Serveradresse des SIEM-Systems**

  IP-Adresse des Servers, auf dem das verwendete SIEM-System installiert ist. Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

- **Serverport des SIEM-Systems**

  Port, über den eine Verbindung zwischen Kaspersky Security Center und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

- **Protokoll**

  Das Protokoll, das für die Übertragung von Daten aus Kaspersky Security Center ins SIEM-System verwendet wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

Über Ereignisse in Kaspersky Security Center

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert. Sie können diese Informationen in externe SIEM-Systeme exportieren. Der Export von Informationen über Ereignisse in externen SIEM-Systeme ermöglicht den Administratoren der SIEM-Systeme, auf die Ereignisse des Sicherheitssystems, die auf den verwalteten Geräten oder in den Administrationsgruppen auftreten, operativ zu reagieren.

Ereignistypen

In Kaspersky Security Center existieren die folgenden Ereignistypen:

- Allgemeine Ereignisse. Diese Ereignisse kommen in allen verwalteten Kaspersky-Anwendungen vor. Als allgemeines Ereignis gilt beispielsweise das Ereignis Virenangriff. Allgemeine Ereignisse haben eine streng definierte Syntax und Semantik. Allgemeine Ereignisse werden beispielsweise in Berichten und auf Dashboards verwendet.

- Spezifische Ereignisse für verwaltete Kaspersky-Anwendungen. Jede verwaltete Kaspersky-Anwendung hat eine eigene Auswahl von Ereignissen.

Quellen von Ereignissen

Ereignisse können von den folgenden Programmen generiert werden:

- Komponenten von Kaspersky Security Center:
  - Administrationsserver
  - Administrationsagent
  - iOS MDM-Server
- Verwaltete Kaspersky-Anwendungen

  Weitere Informationen zu den Ereignissen, die von verwalteten Kaspersky-Programmen generiert werden, finden Sie in der Dokumentation des entsprechenden Programms.

Sie können die vollständige Liste der Ereignisse anzeigen, die von einer Anwendung auf der Registerkarte **Konfiguration von Ereignissen** in der Anwendungsrichtlinie generiert werden können. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen.

Ereigniskategorie von Ereignissen

Jedes Ereignis hat eine eigene Ereigniskategorie. Je nach den Bedingungen des Auftretens, können dem Ereignis verschiedene Ereigniskategorien zugewiesen werden. Es sind vier Ereigniskategorien verfügbar:

- *Kritisches Ereignis* – ein Ereignis, das auf das Auftreten eines kritischen Problems hinweist, das zu Datenverlust, einer Ausführungsstörung oder einem kritischen Fehler führen kann.

- *Funktionsfehler* – das Ereignis, das auf das Auftreten eines ernsten Problems, Fehlers oder einer Störung hinweist, welches während der Ausführung des Programms oder der Prozedur entstanden ist.

- *Warnung* – ein nicht unbedingt ernstes dem Ereignis, das jedoch auf die potentiell mögliche Entstehung eines Problems in der Zukunft hinweist. Meistens gehört die Mehrzahl der Ereignisse zu den Warnungen, wenn nach ihrem Auftreten die Ausführung der Anwendung ohne Datenverlust oder eingeschränkter Funktionalität wiederhergestellt werden kann.

- *Infomeldung* – Ereignis, das zwecks Information über das erfolgreiche Ausführen einer Operation, die korrekte Ausführung des Programms oder den Abschluss einer Prozedur auftritt.

Für jedes Ereignis ist die Speicherdauer festgelegt, die in Kaspersky Security Center angezeigt oder geändert werden kann. Einige Ereignisse werden nicht standardmäßig in der Datenbank des Administrationsservers gespeichert, da die für sie definierte Speicherdauer gleich Null ist. In externe Systeme können nur jene Ereignisse exportieren, die mindestens einen Tag in der Administrationsserver-Datenbank gespeichert werden.

Über den Ereignisexport

Sie können den Ereignisexport innerhalb zentralisierten Systemen verwenden, die sich mit Fragen der Sicherheit auf organisatorischer und technischer Ebene und der Überwachung des Sicherheitssystems beschäftigen sowie Daten aus verschiedenen Lösungen konsolidieren. Dazu gehören SIEM-Systeme, die eine Analyse der Warnungen der Sicherheitssysteme und Ereignisse der Netzwerkhardware und Anwendungen im Echtzeitbetrieb gewährleisten, sowie Security Operation Center (SOC).

Diese Systeme erhalten Daten aus vielen Quellen, einschließlich Netzwerke, Sicherheitssysteme, Server, Datenbanken und Anwendungen. Ferner gewährleisten SIEM-Systeme eine Zusammenfassung der bearbeiteten Daten, damit Sie keine kritischen Ereignisse überspringen können. Außerdem führen diese Systeme eine automatische Analyse der verbundenen Ereignisse und der Alarme zur Benachrichtigung der Administratoren über Fragen des Sicherheitssystems, die eine sofortige Entscheidung fordern, durch. Die Benachrichtigungen können im Indikatorbereich angezeigt oder über dritte Kanäle, beispielsweise E-Mail, versendet werden.

Am Ablauf des Ereignisexports aus Kaspersky Security Center in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Security Center – und der Empfänger der Ereignisse – das SIEM-System. Für einen erfolgreichen Ereignisexport müssen die Einstellungen sowohl im verwendeten SIEM-System als auch in Kaspersky Security Center angepasst werden. Die Reihenfolge der Einstellungen hat keine Bedeutung: Sie können zuerst den Versand der Ereignisse in Kaspersky Security Center und dann das Empfangen der Ereignisse im SIEM-System anpassen oder umgekehrt.

Methoden für den Versand von Ereignissen aus Kaspersky Security Center

Es gibt drei Methoden für den Versand von Ereignisse aus Kaspersky Security Center in die externen Systeme:

- Versand von Ereignissen gemäß dem Protokoll Syslog in ein beliebiges SIEM-System

  Gemäß dem Protokoll Syslog können beliebige Ereignisse, die auf dem Kaspersky Security Center Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, übertragen werden. Das Syslog-Protokoll ist ein Standardprotokoll für das Aufzeichnen von Nachrichten. Sie können es für den Export von Ereignissen ein beliebiges SIEM-System verwenden.

  Zu diesem Zweck müssen Sie die Ereignisse markieren, die Sie an das SIEM-System weiterleiten möchten. Die Ereignisse können Sie in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console markieren. Es werden nur markierte Ereignisse an das SIEM-System weitergeleitet. Wenn Sie nichts markiert haben, werden keine Ereignisse weitergeleitet.

- Versand von Ereignissen gemäß den Protokollen CEF und LEEF in die Systeme QRadar, Splunk und ArcSight

  Sie können die Protokolle CEF und LEEF verwenden, um allgemeine Ereignisse zu exportieren. Die Protokolle CEF und LEEF sind im Gegensatz zum Protokoll Syslog nicht universell. Stattdessen werden alle allgemeinen Ereignisse exportiert. Um Ereignisse von Kaspersky Security Center in Ereignisse im CEF- und LEEF-Format zu konvertieren, können Sie die Datei siem_conversion_rules.xml verwenden. Diese Datei enthält die Liste der Ereignisattribute von Kaspersky Security Center und deren entsprechenden Ereignisattribute im CEF- und LEEF-Format. Zusätzlich enthält die Datei "siem_conversion_rules.xml" Regeln zum Generieren von Nachrichten zu den entsprechenden Ereignissen. Diese Datei ist im Lieferumfang von Kaspersky Security Center enthalten.

  Anders als das Syslog-Protokoll sind das CEF- und das LEEF-Protokoll nicht universell. CEF und LEEF sind für die entsprechenden SIEM-Systeme (QRadar, Splunk und ArcSight) vorgesehen. Wenn Sie daher Ereignisse über eines dieser Protokolle exportieren, verwenden Sie den erforderlichen Parser im SIEM-System.

- Direkt aus der Datenbank von Kaspersky Security Center in ein beliebiges SIEM-System

  Diese Methode für den Ereignisexport kann für das Empfangen von Ereignissen direkt aus den öffentlichen Ansichten der Datenbank mithilfe von SQL-Abfragen verwendet werden. Die Ausführungsergebnisse der Anfrage werden in einer xml-Datei gespeichert und können als Eingangsdaten für das externe System verwendet werden. Nur Ereignisse, die in öffentlichen Ansichten verfügbar sind, können direkt aus der Datenbank exportiert werden.

Empfangen von Ereignissen im SIEM-System

Das SIEM-System muss die von Kaspersky Security Center übertragenen Ereignisse korrekt übernehmen und analysieren. Dazu müssen die Einstellungen des SIEM-Systems angepasst werden. Die Konfiguration hängt vom verwendeten speziellen SIEM-System ab. Es gibt jedoch eine Anzahl von allgemeinen Schritten in der Konfiguration aller SIEM-Systeme, etwa die Konfiguration des Empfängers und des Parsers.

Über das Konfigurieren des Ereignisexports in ein SIEM-System

Am Ablauf des Ereignisexports aus Kaspersky Security Center in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Security Center – und der Empfänger der Ereignisse – das SIEM-System. Der Ereignisexport wird im verwendeten SIEM-System und in Kaspersky Security Center angepasst.

Die Einstellungen, die im SIEM-System vorgenommen werden, sind vom System abhängig, das Sie verwenden. Im Allgemeinen müssen für alle SIEM-Systeme der Empfänger der Nachrichten und, falls erforderlich, der Nachrichtenparser angepasst werden, damit die erhaltenen Nachrichten auf die Felder verteilt werden können.

Einstellungen des Empfängers der Nachrichten

Für das SIEM-Systems muss der Empfänger für den Erhalt der Ereignisse, die von Kaspersky Security Center gesendet werden, angepasst werden. Im Allgemeinen müssen im SIEM-System die folgenden Einstellungen angegeben werden:

- **Exportprotokoll oder Typ der Eingangsdaten**

  Dies ist das Protokoll zum Übertragen von Nachrichten, beispielsweise UDP. Das Protokoll muss das dasselbe Protokoll sein, das Sie in Kaspersky Security Center angegeben haben.

- **Port**

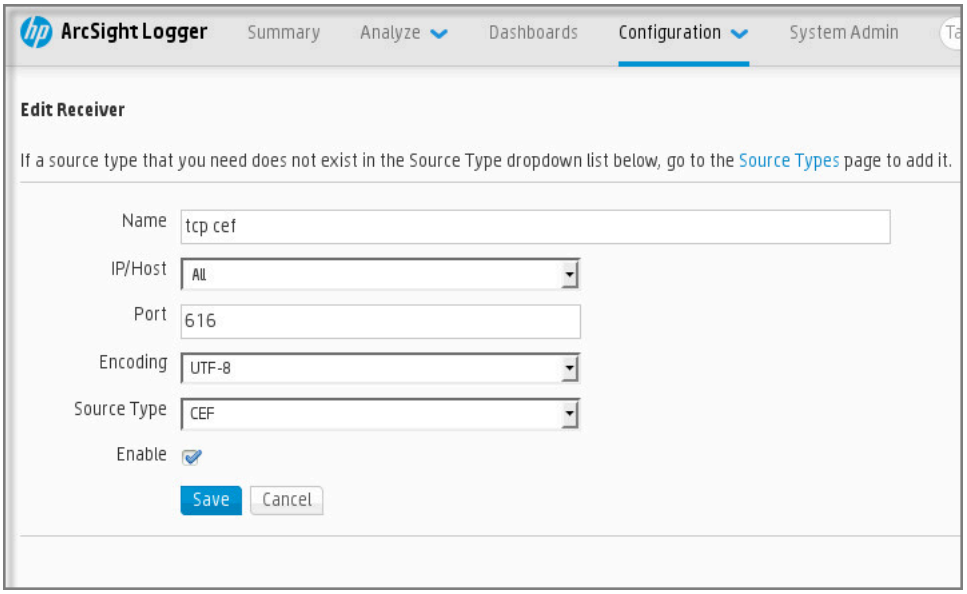
  Port für die Verbindung mit Kaspersky Security Center. Es muss derselbe Port angegeben werden, der in Kaspersky Security Center für die Übertragung der Ereignisse ausgewählt war.

- **Übertragungsprotokoll der Nachrichten oder Typ der Quelldaten**

  Protokoll für den Ereignisexport in das SIEM-System Es kann eines der Standardprotokolle sein: Syslog, CEF oder LEEF. Das SIEM-System wählt den Nachrichtenparser gemäß dem angegebenen Protokoll aus.

Je nachdem, welches SIEM-System Sie verwendetem, kann es erforderlich sein, erweiterte Einstellungen für den Empfänger der Nachrichten anzugeben.

Auf der unteren Abbildung dienen die Einstellungen des Empfängers in ArcSight als Beispiel.



Einstellungen des Empfängers in ArcSight

Nachrichtenparser

Die exportierten Ereignisse werden in Form von Nachrichten an das SIEM-System übergeben. Dann wird für diese Nachrichten der Parser verwendet, damit die Informationen über die Ereignisse entsprechend ins SIEM-System übergeben werden. Die Nachrichtenparser sind im SIEM-System integriert und werden für die Aufteilung der Nachrichten in Felder wie Nachrichten-ID, Signifikanz, Beschreibung und Parameter verwendet. Daraufhin hat das SIEM-System die Möglichkeit, die Ereignisse, die aus Kaspersky Security Center empfangen werden, so zu verarbeiten, dass sie in der Datenbank des SIEM-Systems gespeichert werden.

Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren

Nach der Aktivierung des automatischen Ereignisexports müssen Sie auswählen, welche Ereignisse ins externe SIEM-System exportiert werden sollen.

Sie können den Ereignisexport in das Syslog-Format in ein externes System gemäß einer der folgenden Bedingungen anpassen:

- Allgemeine Ereignisse markieren. Wenn Sie die zu exportierenden Ereignisse in der Richtlinie, in den Einstellungen eines Ereignisses oder in den Einstellungen des Administrationsservers markieren, erhält das SIEM-System die ausgewählten Ereignisse, die in allen Anwendungen auftreten, die von der Richtlinie verwaltet werden. Falls die zu exportierenden Ereignisse in der Richtlinie ausgewählt worden sind, ist es unmöglich, diese für eine einzelne Anwendung, die von dieser Richtlinie verwaltet wird, umzudefinieren.

- Ereignisse für eine verwaltete Anwendung markieren. Wenn Sie die zu exportierenden Ereignisse für eine verwaltete Anwendungen auf einem verwalteten Gerät markieren, werden nur Ereignisse in das SIEM-System übertragen, die in dieser Anwendung aufgetreten sind.

Ereignisse von Kaspersky-Anwendungen für den Export im Syslog-Format markieren

Wenn Sie Ereignisse exportieren möchten, die in einem einzelnen verwalteten Programm, welches auf einem einzelnen verwalteten Gerät installiert ist, auftreten, markieren Sie für das Programm die Ereignisse für den Export aus. Falls die zu exportierenden Ereignisse früher in der Richtlinie markiert worden sind, ist es unmöglich, die markierten Ereignisse für ein einzelnes Programm, das von dieser Richtlinie verwaltet wird, neu zu definieren.

Um die zu exportierenden Ereignisse für ein einzelnes verwaltetes Programm zu markieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur von Kaspersky Security Center den Knoten **Verwaltete Geräte** aus und wechseln Sie zur Registerkarte **Geräte**.

2. Öffnen Sie mit der rechten Maustaste das Kontextmenü des gewünschten Geräts und wählen Sie den Punkt **Eigenschaften** aus.

3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts den Abschnitt **Programme** aus.

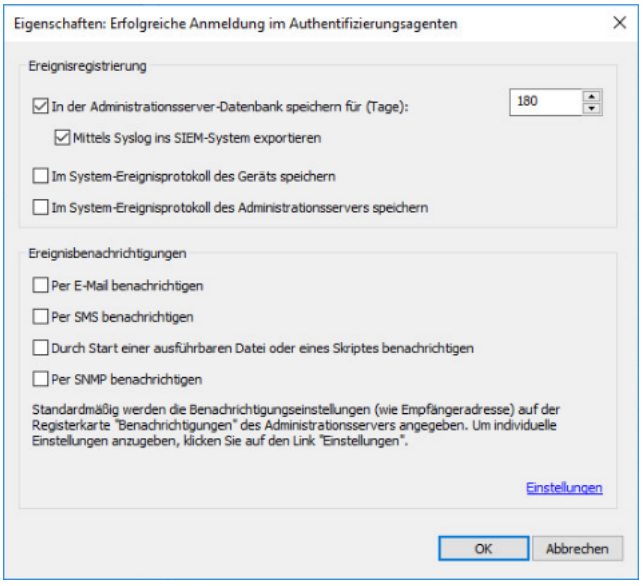
4. Wählen Sie in der angezeigten Programmliste das Programm aus, dessen Ereignisse exportiert werden sollen, und klicken Sie auf die Schaltfläche **Eigenschaften**.

5. Wählen Sie im Eigenschaftenfenster des Programms den Abschnitt **Konfiguration von Ereignissen** aus.

6. Wählen Sie in der angezeigten Ereignisliste ein oder mehrere Ereignisse aus, die ins SIEM-System exportiert werden sollen, und klicken Sie auf die Schaltfläche **Eigenschaften**.

7. Aktivieren Sie im angezeigten Fenster mit den Ereigniseigenschaften das Kontrollkästchen **Mittels Syslog in ein SIEM-System exportieren**, um die ausgewählten Ereignisse für den Export im Syslog-Format zu markieren. Deaktivieren Sie das Kontrollkästchen **Mittels Syslog in ein SIEM-System exportieren**, um die Markierung der ausgewählten Ereignisse für den Export in das Syslog-Format aufzuheben.

   Wenn die Eigenschaften des Ereignisses in der Richtlinie festgelegt sind, können die Felder dieses Fensters nicht bearbeitet werden.



Fenster "Eigenschaften des Ereignisses"

8. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

9. Klicken Sie im Eigenschaftenfenster des Programms und im Eigenschaftenfenster des Geräts auf die Schaltfläche **OK**.

Die markierten Ereignisse werden über das Syslog-Format ins SIEM-System übertragen. Die Ereignisse, für welche Sie das Kontrollkästchen **Mittels Syslog in ein SIEM-System exportieren** deaktiviert haben, werden nicht in ein SIEM-System exportiert. Der Export beginnt sofort, nachdem Sie den automatischen Export aktiviert und die zu exportierenden Ereignisse ausgewählt haben. Konfigurieren Sie die Einstellungen auf der Seite des SIEM-Systems, um das Empfangen von Ereignissen aus Kaspersky Security Center sicherzustellen.

Allgemeine Ereignisse für den Export in das Syslog-Format markieren

Wenn Sie Ereignisse exportieren möchten, die in allen Programmen aufgetreten sind, die von einer bestimmten Richtlinie verwaltet werden, markieren Sie die zu exportierenden Ereignisse in der Richtlinie aus. In diesem Fall können keine Ereignisse für einzelne verwaltete Programme markiert werden.

So markieren Sie Ereignisse für den Export in ein SIEM-System:

1. Wählen Sie in der Konsolenstruktur von Kaspersky Security Center den Knoten **Richtlinien** aus.

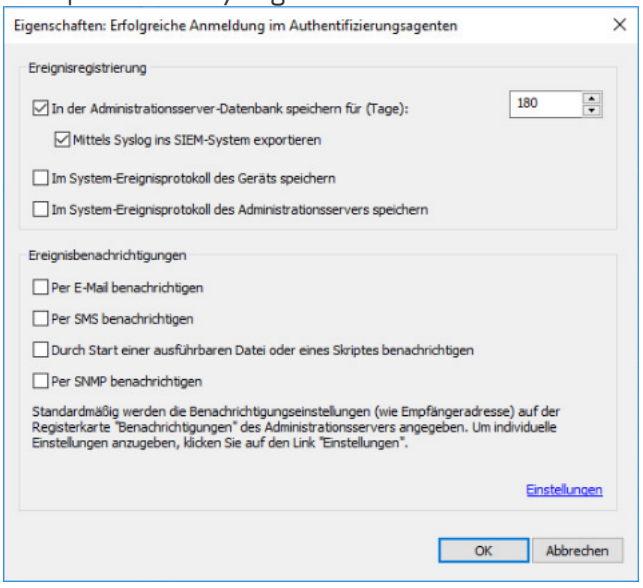
2. Öffnen Sie mit der rechten Maustaste das Kontextmenü der gewünschten Richtlinie und wählen Sie den Punkt **Eigenschaften** aus.

3. Wählen Sie im folgende Eigenschaftenfenster der Richtlinie den Abschnitt **Konfiguration von Ereignissen** aus.

4. Wählen Sie in der angezeigten Ereignisliste ein oder mehrere Ereignisse aus, die ins SIEM-System exportiert werden sollen, und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Wenn es erforderlich ist, alle Ereignisse auszuwählen, klicken Sie auf die Schaltfläche **Alle auswählen**.

5. Aktivieren Sie im angezeigten Fenster mit den Ereigniseigenschaften das Kontrollkästchen **Mittels Syslog in ein SIEM-System exportieren**, um die ausgewählten Ereignisse für den Export im Syslog-Format zu markieren. Deaktivieren Sie das Kontrollkästchen **Mittels Syslog in ein SIEM-System exportieren**, um die Markierung der ausgewählten Ereignisse für den Export in das Syslog-Format aufzuheben.



Eigenschaftenfenster der Ereignisse des Administrationsservers

6. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

7. Klicken Sie im Eigenschaftenfenster der Richtlinie auf die Schaltfläche **OK**.

Die markierten Ereignisse werden über das Syslog-Format ins SIEM-System übertragen. Die Ereignisse, für welche Sie das Kontrollkästchen **Mittels Syslog in ein SIEM-System exportieren** deaktiviert haben, werden nicht in ein SIEM-System exportiert. Der Export beginnt sofort, nachdem Sie den automatischen Export aktiviert und die zu exportierenden Ereignisse ausgewählt haben. Konfigurieren Sie die Einstellungen auf der Seite des SIEM-Systems, um das Empfangen von Ereignissen aus Kaspersky Security Center sicherzustellen.

Über das Exportieren von Ereignissen im Syslog-Format

Gemäß dem Syslog-Format können Ereignisse, die auf dem Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, ins SIEM-System exportiert werden.

Syslog ist ein Standardprotokoll zur Registrierung von Nachrichten. Dieses Protokoll ermöglicht, die Software, in der die Nachrichten generiert werden, das System, in dem die Nachrichten gespeichert werden, und die Software, in der die Analysen und die Berichterstellung für die Nachrichten ausgeführt wird, zu trennen. Jeder Nachricht wird der Code des Geräts, der den Typ der Software angibt, mit dessen Hilfe die Nachricht erstellt wurde, und die Signifikanz zugewiesen.

Das Syslog-Format wird in den Dokumenten "Request for Comments" (RFC) definiert, die von der Internet Engineering Task Force veröffentlicht werden. Der Standard RFC 5424 wird für den Ereignisexport aus Kaspersky Security Center in externe Systeme verwendet.

n Kaspersky Security Center können Sie den Ereignisexport in externe Systeme gemäß dem Syslog-Format anpassen.

Der Ablauf des Exports besteht aus zwei Schritten:

1. Aktivierung des automatischen Ereignisexports. In diesem Schritt werden die Einstellungen von Kaspersky Security Center so angepasst, dass der Versand von Ereignissen ins SIEM-System ausgeführt werden kann. Der Versand von Ereignissen aus Kaspersky Security Center beginnt sofort nach der Aktivierung des automatischen Exports.

2. Auswahl der Ereignisse, die ins externe System exportiert werden sollen. In diesem Schritt müssen Sie auswählen, welche Ereignisse ins SIEM-System exportiert werden sollen.

Über das Exportieren von Ereignissen mittels der Formate CEF und LEEF

Die CEF- und LEEF-Formate können verwendet werden, um allgemeine Ereignisse und Ereignisse, die von Kaspersky-Anwendungen an den Administrationsserver übertragen werden, in SIEM-Systeme zu exportieren. Der Satz der zu exportierenden Ereignisse ist vordefiniert, es gibt keine Möglichkeit, die zu exportierenden Ereignisse auszuwählen. Bevor Ereignisse aus Kaspersky Security Center an ein SIEM-System (QRadar, ArcSight oder Splunk) übertragen werden können, müssen diese Ereignisse in das CEF- oder LEEF-Format konvertiert werden. Dies geschieht unter Verwendung der Regeln, die in der Datei siem_conversion_rules.xml enthalten sind.

Das Exportformat kann abhängig vom verwendeten SIEM-System ausgewählt werden. In der folgenden Tabelle sind die SIEM-Systeme und die ihnen entsprechenden Exportformate angeführt.

Formate für den Ereignisexport in ein SIEM-System

SIEM-System	Exportformat
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) ist ein spezielles Format für Ereignisprotokollierung in IBM Security QRadar SIEM. QRadar kann Ereignisse, die gemäß dem LEEF-Protokoll übergeben werden, sammeln, identifizieren und bearbeiten. Für das LEEF-Protokoll muss die UTF-8-Kodierung verwendet werden. Ausführlicheren Informationen über das LEEF-Protokoll finden Sie im IBM Knowledge Center.

- CEF ist ein Standard der Verwaltung vom Typ "offenes Protokoll", der die Kompatibilität der Informationen des Sicherheitssystems verschiedener Netzwerkgeräte und Apps verbessert. Das CEF-Protokoll ermöglicht die Verwendung eines allgemeinen Formats für das Ereignisprotokoll, damit die Managementsysteme für Unternehmen die Daten für die Analyse problemlos abrufen und zusammenfassen können. Für das CEF-Protokoll muss die UTF-8-Kodierung verwendet werden.

Automatischer Export bedeutet, dass Kaspersky Security Center die allgemeinen Ereignisse ins SIEM-System sendet. Der automatische Export der Ereignisse beginnt sofort nach der Aktivierung. In diesem Abschnitt ist der Ablauf zur Aktivierung des automatischen Exports von Ereignissen beschrieben.

Konfiguration von Kaspersky Security Center für den Export an ein SIEM-System

Sie können in Kaspersky Security Center den automatischen Ereignisexport aktivieren.

Mit den Formaten CEF und LEEF können nur allgemeine Ereignisse aus verwalteten Programmen exportiert werden. Die zur Konvertierung von Ereignissen in das CEF- und LEEF-Format verwendeten Interpretationsregeln sind in der Datei siem_conversion_rules.xml angegeben, die im Lieferumfang von Kaspersky Security Center enthalten ist. Programmspezifische Ereignisse können mit den Formaten CEF und LEEF nicht aus verwalteten Programmen exportiert werden. Wenn es erforderlich ist, die Ereignisse der verwalteten Programme oder einen benutzerdefinierten Satz von Ereignissen, der mit der Hilfe der Richtlinien der verwalteten Programme angepasst wurde, zu exportieren, müssen Sie die Ereignisse im Syslog-Format exportieren.

So aktivieren Sie den automatischen Export von Ereignissen:

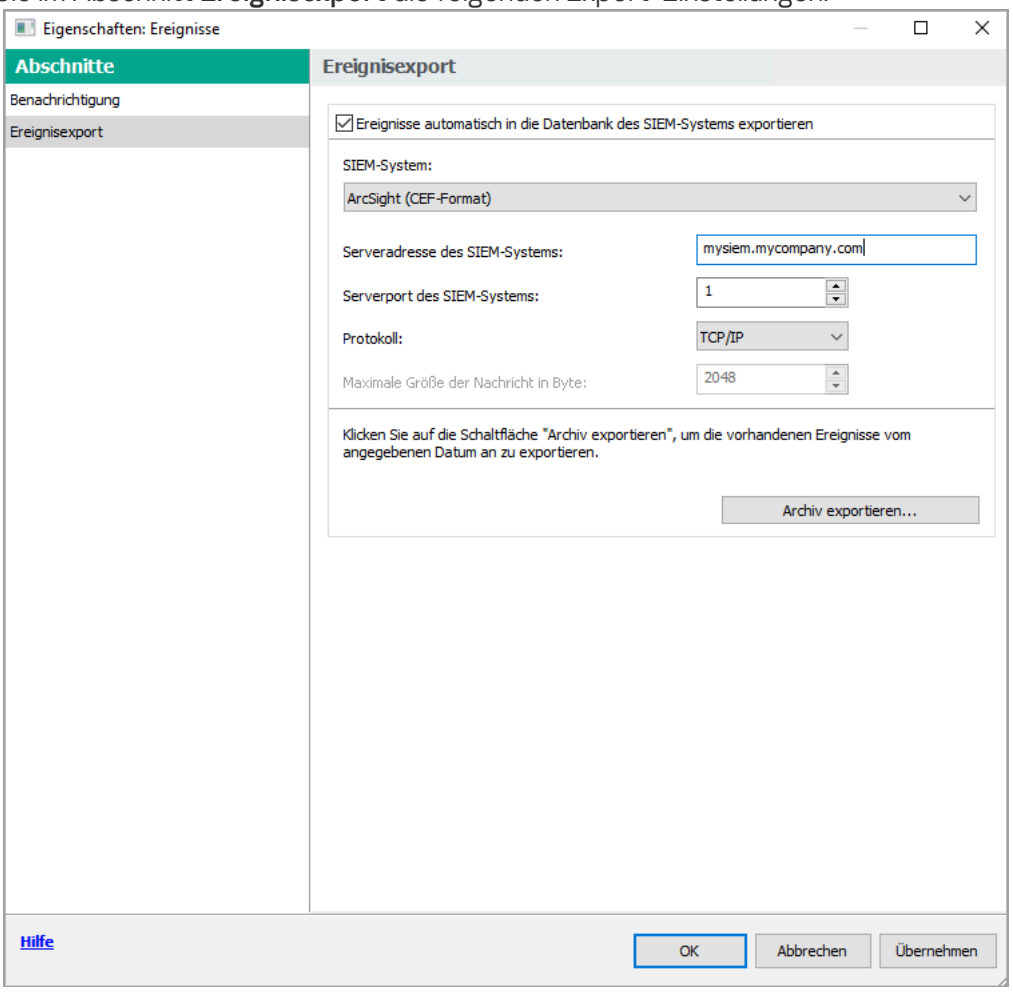
1. Wählen Sie im Konsolenbaum von Kaspersky Security Center den Knoten mit dem Namen des Administrationsservers aus, dessen Ereignisse exportiert werden sollen.

2. Wählen Sie im Arbeitsbereich des ausgewählten Administrationsservers die Registerkarte **Ereignisse** aus.

3. Klicken Sie auf den Dropdown-Pfeil neben dem Link **Benachrichtigungseinstellungen und Ereignis-Export anpassen** und wählen Sie anschließend in der Dropdown-Liste den Punkt **Export in ein SIEM-System anpassen** aus.

   Das Eigenschaftenfenster für Ereignisse wird im Abschnitt **Ereignisexport** geöffnet.

4. Konfigurieren Sie im Abschnitt **Ereignisexport** die folgenden Export-Einstellungen:



Abschnitt "Ereignisexport" des Eigenschaftsfensters für Ereignisse

- **Ereignisse automatisch in die Datenbank des SIEM-Systems exportieren**

  Aktivieren Sie dieses Kontrollkästchen, um den automatischen Ereignisexport ins SIEM-System zu aktivieren. Nach der Aktivierung dieses Kontrollkästchens können alle Felder im Abschnitt **Ereignisexport** bearbeitet werden.

- **SIEM-System**

  Wählen Sie das SIEM-System aus, um folgende Ereignisse zu exportieren: QRadar® (LEEF-Format), ArcSight (CEF-Format), Splunk® (CEF-Format) und Syslog-Format (RFC 5424).

  Wenn Sie das Syslog-Format auswählen, müssen Sie folgendes angeben:

  Maximale Größe der Nachricht in Byte

  Geben Sie die maximale Größe der Nachricht in Byte an, die an das SIEM-System übertragen wird. Jedes Ereignis wird in einer Nachricht übermittelt. Wenn die reale Länge der Nachricht den angegebenen Wert überschreitet, wird die Nachricht abgeschnitten und Daten können verloren gehen. Standardmäßig beträgt die Größe der Nachricht 2048 Bytes. Dieses Feld ist nur verfügbar, falls Sie im Feld **SIEM-System** das Format Syslog ausgewählt haben.

- **Serveradresse des SIEM-Systems**

  Geben Sie die Serveradresse des SIEM-Systems an. Die Serveradresse kann im Format DNS- oder NetBIOS-Name oder als IP-Adresse angegeben werden.

- **Serverport des SIEM-Systems**

  Geben Sie den Port für die Verbindung mit dem Server des SIEM-Systems an. Dieser Port muss mit dem Port übereinstimmen, den Sie in den Einstellungen des Empfängers des SIEM-Systems für das Empfangen von Ereignissen (s. Abschnitt "Einstellungen des SIEM-Systems") angegeben haben.

- **Protokoll**

  Wählen Sie das Übertragungsprotokoll für Nachrichten ins SIEM-System aus. Sie können das TCP-, UDP- oder TLS-over-TCP-Protokoll auswählen.

  Wenn Sie das Protokoll TLS over TCP auswählen, geben Sie die folgenden TLS-Einstellungen an:

  - **Authentifizierung des SIEM-Servers**

    Wählen Sie eine der folgenden Möglichkeiten, um den SIEM-Systemserver zu authentifizieren:

    - **Durch CA-Zertifikate**. Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority – CA) enthält, und diese Datei in Kaspersky Security Center hochladen. Kaspersky Security Center prüft, ob das Zertifikat des SIEM-Servers auch von einer vertrauenswürdigen CA signiert ist oder nicht.

      Um ein vertrauenswürdiges Zertifikat hinzuzufügen, klicken Sie auf die Schaltfläche **Durchsuchen** und laden Sie anschließend das Zertifikat hoch.

      Wenn Sie die Option **Durch CA-Zertifikate** ausgewählt haben, können Sie den Antragstellernamen im Feld **Antragsteller der Serverzertifikate (optional)** angeben. Der *Antragstellername* ist ein Domänenname, für den das Zertifikat empfangen wird. Kaspersky Security Center kann keine Verbindung zu dem SIEM-System-Server herstellen, wenn der Domänenname des SIEM-System-Servers nicht mit dem Antragstellernamen des Zertifikats des SIEM-System-Servers übereinstimmt. Der SIEM-Systemserver kann jedoch seinen Domänennamen ändern, wenn Sie den Namen des Antragstellers im Zertifikat ändern. Geben Sie dazu die Antragstellernamen im Feld **Antragsteller der Serverzertifikate (optional)** an. Wenn einer der angegebenen Antragstellernamen mit dem Antragsteller des Zertifikats für das SIEM-Systems übereinstimmt, validiert Kaspersky Security Center das Zertifikat dieses SIEM-Systems.

    - **Durch SHA1-Fingerabdrücke von Serverzertifikaten**. In Kaspersky Security Center können Sie die SHA-1-Fingerabdrücke der Zertifikate von SIEM-Systemen angeben. Um einen SHA-1-Fingerabdruck hinzuzufügen, geben Sie ihn in das Feld unter der Option ein.

  - **Client-Authentifizierung**

Um die Client-Authentifizierung durchzuführen, können Sie entweder Ihr Zertifikat einfügen oder es im Kaspersky Security Center generieren.

- **Zertifikat einfügen**. Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen CA. Um ein vorhandenes Zertifikat einzufügen, klicken Sie auf die Schaltfläche **Zertifikat auswählen**. Wählen Sie im geöffneten Fenster **Zertifikat** einen der folgenden Zertifikatstypen aus und geben Sie dann das Zertifikat und seinen privaten Schlüssel an:

  - **X.509-Zertifikat**. Laden Sie jeweils eine Datei mit einem privaten Schlüssel im Feld **Privater Schlüssel (*.prk, *.pem)** hoch und eine Datei mit einem Zertifikat im Feld **Zertifikat (*.cer)**. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** rechts neben dem entsprechenden Feld und fügen Sie dann die gewünschte Datei hinzu. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Hochladen der Dateien ist spielt keine Rolle. Geben Sie nach dem Hochladen beider Dateien das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Kennwort** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

  - **Container PKCS#12**. Laden Sie in dem Feld **Zertifikatdatei** eine Datei hoch, die ein Zertifikat und dessen privaten Schlüssel enthält. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** rechts neben dem Feld und fügen Sie dann die erforderliche Datei hinzu. Geben Sie nach dem Hochladen der Datei das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Kennwort** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- **Schlüssel generieren**. Sie können in Kaspersky Security Center ein selbstsigniertes Zertifikat generieren. Klicken Sie auf die Schaltfläche **Zertifikat erstellen** und geben Sie anschließend einen Antragstellernamen in das ein Feld **Antragsteller** ein. Das Client-Zertifikat wird für diesen Antragstellernamen generiert und der SHA-1-Fingerabdruck dieses Zertifikats wird im Feld **SHA1-Fingerabdruck des Client-Zertifikats** angezeigt. Infolge dessen speichert Kaspersky Security Center das generierte selbstsignierte Zertifikat und Sie können den öffentlichen Teil des Zertifikats oder den SHA-1-Fingerabdruck an das SIEM-System übergeben.

5. Wenn es erforderlich ist, Ereignisse, die nach einem bestimmten Datum in der Vergangenheit aufgetreten sind, in ein SIEM-System zu exportieren, klicken Sie auf die Schaltfläche **Archiv exportieren** und geben Sie anschließend das Datum an, ab dem der Export der Ereignisse ausgeführt werden soll. Standardmäßig beginnt der Export der Ereignisse sofort nach der Aktivierung.

6. Um zu überprüfen, ob die Verbindung mit dem SIEM-System konfiguriert wurde, klicken Sie auf die Schaltfläche **Verbindung testen**.

   Die Anwendung versucht, eine Verbindung mit dem Server des SIEM-Systems herzustellen und ein Testereignis zu senden. Wenn die Verbindung nicht erstellt wurde, wird eine Fehlermeldung angezeigt. Wenn die Verbindung erstellt wurde, wird keine Meldung angezeigt. Sie können das Resultat des Tests bei Bedarf auf der Registerkarte **Ereignisse** anzeigen.

7. Klicken Sie auf die Schaltfläche **OK**.

Der automatische Ereignisexport ist aktiviert.

Nach der Aktivierung des automatischen Ereignisexports müssen Sie auswählen, welche Ereignisse ins SIEM-System exportiert werden sollen.

Ereignisexport direkt aus der Datenbank

Sie können die Ereignisse direkt aus der Datenbank Kaspersky Security Center extrahieren, ohne die Benutzeroberfläche von Kaspersky Security Center zu verwenden. Die Abfragen können unmittelbar in Bezug auf die öffentlichen Ansichten erstellt und von daraus Daten über die Ereignisse extrahiert werden, oder Sie können eigene Ansichten auf der Grundlage der vorhandenen öffentlichen Ansichten erstellen und die gewünschten Daten von dort beziehen.

Öffentlichen Ansichten

Zur Erhöhung der Benutzerfreundlichkeit sind in der Datenbank von Kaspersky Security Center ein Satz öffentlicher Ansichten vorgesehen. Eine Beschreibung der öffentlichen Ansichten finden Sie im Dokument klakdb.chm.

Die öffentliche Ansicht v_akpub_ev_event enthält einen Satz Felder, die den Einstellungen der Ereignisse in der Datenbank entsprechen. Im Dokument klakdb.chm finden Sie Informationen über die öffentlichen Ansichten, die sich auf andere Objekte von Kaspersky Security Center beziehen, beispielsweise Geräte, Programme, Benutzer. Sie können diese Informationen beim Erstellen von Abfragen verwenden.

In diesem Abschnitt finden Sie Anweisungen zum Ausführen einer SQL-Abfrage mithilfe des Tools "klsql2" sowie eine Beispielabfrage.

Sie können auch beliebige andere Datenbankenanwendungen für das Erstellen der SQL-Abfragen und die Datenbankenansichten verwenden. Informationen zur Anzeige der Verbindungseinstellungen der Datenbank von Kaspersky Security Center, wie z. B. Instanz-Name und Name der Datenbank, finden Sie im entsprechenden Abschnitt.

Eine SQL-Abfrage mit dem Tool "klsql2" ausführen

In diesem Artikel erhalten Sie Anweisungen zum Herunterladen und für die Nutzung des Tools klsql2 sowie zum Ausführen einer SQL-Abfrage mithilfe dieses Tools.

So verwenden Sie das Tool "klsql2":

1. Navigieren Sie zum Tool "klsrvswch" im Installationsordner von Kaspersky Security Center. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center". Verwenden Sie keine Versionen des Tools "klsql2", die für ältere Versionen von Kaspersky Security Center bestimmt sind.

2. Erstellen Sie in einem beliebigen Texteditor eine Datei mit sql-Endung und legen Sie die Datei im selben Ordner wie das Tool ab.

3. Geben Sie den von Ihnen gewünschten SQL-Query in die erstellte sql-Datei ein und speichern Sie die Datei.

4. Geben Sie auf dem Gerät, auf dem der Kaspersky Security Center Administrationsserver installiert ist, in der Befehlszeile den folgenden Befehl für die Ausführung der SQL-Abfrage aus der sql-Datei und zur Speicherung der Ergebnisse in der Datei "result.xml" ein:

   ```
   klsql2 -i src.sql -u <Benutzername> -p <Kennwort> -o result.xml
   ```

   Wobei `<Benutzername>` und `<Kennwort>` den Anmeldeinformationen des Benutzerkontos entsprechen, das Zugriff auf die Datenbank hat.

5. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des Benutzerkontos ein, das Zugriff auf die Datenbank hat.

6. Öffnen Sie die neu erstellten Dateien des Typs "result.xml" und sehen Sie sich die Ergebnisse der SQL-Abfragen an.

Sie können die sql-Datei editieren und darin beliebige SQL-Anfragen an öffentliche Ansichten erstellen. Führen Sie anschließend in der Befehlszeile Ihre SQL-Abfrage aus und speichern Sie das Ergebnis in einer Datei.

Beispiel einer SQL-Abfrage, die mit dem Tool "klsql2" erstellt wurde

Dieser Abschnitt enthält eine beispielhafte SQL-Anfrage, die mittels des Tools "klsql2" ausgeführt wurde.

Die folgenden Beispiele zeigen, wie Sie eine Liste mit den Ereignissen auf den Benutzergeräten für die letzten sieben Tage abrufen und diese nach ihrem Eintrittszeitpunkt sortieren. Die aktuellsten Ereignisse werden zuerst angezeigt.

Beispiel für Microsoft SQL Server:

```
SELECT
  /* ID des Ereignisses */
  e.nId,

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  e.tmRiseTime,

  /* interner Name des Ereignistyps */
  e.strEventType,

  /* angezeigter Name des Ereignisses */
  e.wstrEventTypeDisplayName,

  /* angezeigte Beschreibung des Ereignisses */
  e.wstrDescription,

  /* Name der Gruppe, in der sich das Gerät befindet */
  e.wstrGroupName,

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Beispiel für PostgreSQL:

```
SELECT
  /* ID des Ereignisses */
  "e"."nId",

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  "e"."tmRiseTime",

  /* interner Name des Ereignistyps */
  "e"."strEventType",

  /* angezeigter Name des Ereignisses */
  "e"."wstrEventTypeDisplayName",

  /* angezeigte Beschreibung des Ereignisses */
  "e"."wstrDescription",

  /* angezeigte Beschreibung des Ereignisses */
  "e"."wstrGroupName",

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Beispiel für MySQL oder MariaDB

```
SELECT

  /* ID des Ereignisses */
  `e`.`nId`,

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  `e`.`tmRiseTime`,

  /* interner Name des Ereignistyps */
  `e`.`strEventType`,

  /* angezeigter Name des Ereignisses */
  `e`.`wstrEventTypeDisplayName`,

  /* angezeigte Beschreibung des Ereignisses */
  `e`.`wstrDescription`,

  /* Name der Gerätegruppe */
  `e`.`wstrGroupName`,

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Anzeige des Namens der Datenbank von Kaspersky Security Center

Es kann hilfreich sein, einen Datenbanknamen zu kennen, wenn Sie beispielsweise eine SQL-Abfrage senden müssen und von Ihrem SQL-Skripteditor aus eine Verbindung zur Datenbank herstellen wollen.

Um den Namen der Datenbank von Kaspersky Security Center anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie den Punkt **Eigenschaften** aus.

2. Wählen Sie im Auswahlbereich des Fensters "Eigenschaften des Administrationsservers" die Option **Erweitert** und anschließend **Details der aktuellen Datenbank** aus.

3. Beachten Sie im Abschnitt **Details der aktuellen Datenbank** die folgenden Eigenschaften der Datenbank (siehe Abb. unten):

   - **Instanzname**

     Name der aktuellen Datenbankinstanz von Kaspersky Security Center. Der Standardwert lautet *.\KAV_CS_ADMIN_KIT.*

   - **Name der Datenbank**

     Name der SQL-Datenbank von Kaspersky Security Center Standardmäßig ist der Wert auf *KAV* eingestellt.

   - **Zugewiesener Speicherplatz für die Datenbank**

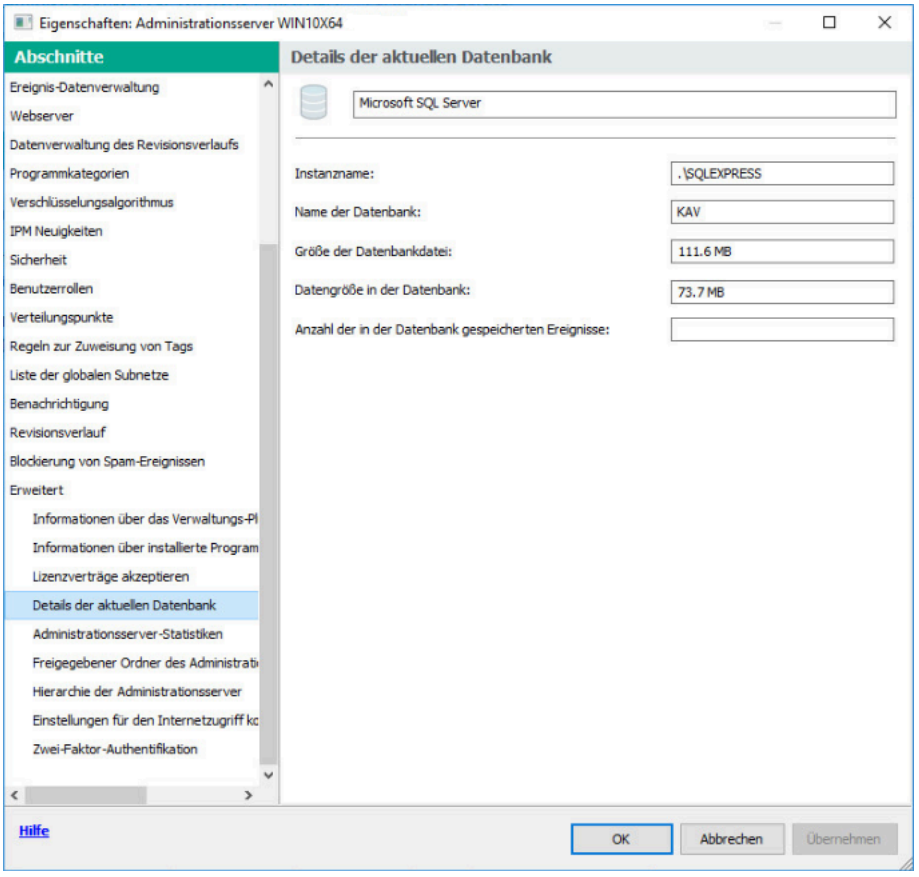
     Die Größe der Datenbankdatei. Wenn Sie unnötige Daten bereinigen möchten, konfigurieren Sie die Komprimierung der Datenbank mithilfe der Aufgabe *Wartung des Administrationsservers*.

   - **Größe der Daten in der gesamten Datenbank**

     Die tatsächliche Größe der derzeit im DBMS verwendeten Daten. Der folgende Artikel beschreibt die DBMS-Diagnose: Datenbankgröße überschreitet das Limit.

- **Anzahl der in der Datenbank gespeicherten Ereignisse**

  Die Anzahl der Ereignisse, die derzeit im DBMS gespeichert sind. Mehr Informationen dazu finden Sie im folgenden Artikel: Verarbeitung und Speicherung von Ereignissen.



Abschnitt "Informationen über verwendete Administrationsserver-Datenbank"

4. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Administrationsservers zu schließen.

Verwenden Sie diesen Namen der Datenbank für die Verbindung und den Zugriff auf die Datenbank in Ihren SQL-Abfragen.

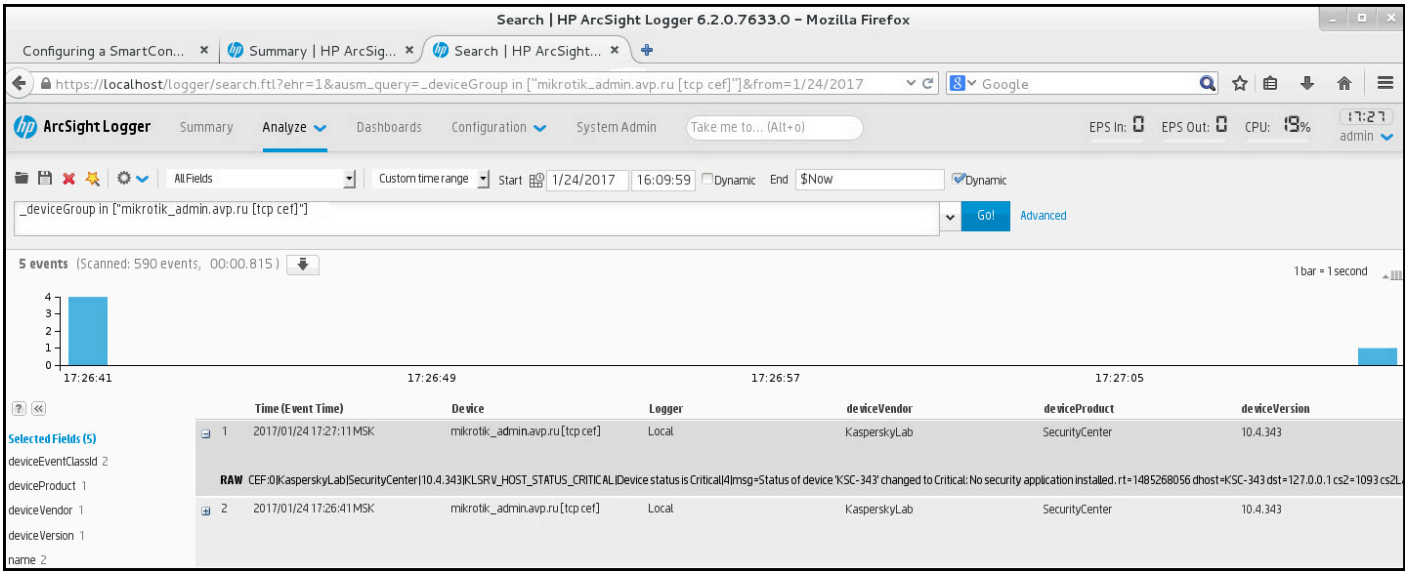
Exportergebnisse anzeigen

Sie können erfahren, ob die Exportprozedur erfolgreich fertig gestellt wurde. Überprüfen Sie dazu, ob das SIEM-System die Nachrichten, in denen die exportierten Ereignisse enthalten sind, erhalten hat.

Wenn die aus Kaspersky Security Center versendeten Ereignisse erhalten und vom SIEM-System richtig interpretiert wurden, bedeutet das, dass die Einstellungen auf beiden Seiten korrekt ausgeführt wurden. Andernfalls prüfen Sie und korrigieren Sie erforderlichenfalls die Einstellungen in Kaspersky Security Center und im SIEM-Systeme.

Nachfolgend finden Sie ein Beispiel für Ereignisse, die ins ArcSight-System exportiert wurden. Das erste Ereignis ist beispielsweise ein kritisches Ereignis des Administrationsservers: "*Gerätestatus ist Kritisch*".

Die Anzeige der exportierten Ereignisse ist vom verwendeten SIEM-System abhängig.



Beispiel für Ereignisse

Verwenden von SNMP zum Senden von Statistiken an Programme von Drittanbietern

In diesem Abschnitt wird beschrieben, wie Sie mithilfe von SNMP (Simple Network Management Protocol) unter Windows Informationen vom Administrationsserver abrufen. Kaspersky Security Center enthält einen SNMP-Agenten, der mithilfe von OIDs Statistiken zur Leistung des Administrationsservers an Nebenprogramme überträgt.

Dieser Abschnitt enthält auch Informationen zur Behebung von Problemen, die bei der Verwendung von SNMP für Kaspersky Security Center auftreten können.

Den SNMP-Dienst für die Verwendung mit Kaspersky Security Center konfigurieren

In diesem Abschnitt wird beschrieben, wie der SNMP-Dienst unter Windows so konfiguriert wird, dass mithilfe des Simple Network Management Protocol (SNMP) Informationen vom Administrationsserver abgerufen werden können.

Die SNMP-Unterstützung ist in Windows standardmäßig deaktiviert.

So aktivieren Sie die SNMP-Unterstützung in Windows:

1. Navigieren Sie zur **Systemsteuerung**.
2. Öffnen Sie das Menü **Programme und Features**.
3. Klicken Sie auf **Windows-Features aktivieren oder deaktivieren**.
4. Navigieren Sie in der Liste der Windows-Features zur SNMP-Funktion und klicken Sie dann auf **OK**.

5. Navigieren Sie zu **Systemsteuerung** → **Alle Systemsteuerungselemente – Verwaltung** → **Dienste**.

6. Wählen Sie den **SNMP-Dienst** und führen Sie ihn aus.

7. Überprüfen Sie, ob der Dienst am Port wartet, indem Sie einen Test mit `netstat` auf einem Standard-UDP-Port durchführen.

Die SNMP-Unterstützung ist unter Windows aktiviert.

So konfigurieren Sie die SNMP-Dienste unter Windows:

1. Stellen Sie sicher, dass die Komponente **SNMP-Agent** im Rahmen der regulären Installation oder der Installation im Silent-Modus von Kaspersky Security Center installiert wurde.

2. Stellen Sie sicher, dass die Windows-Dienste **SNMP Service** und **SNMP Trap** ausgeführt werden.

3. Stellen Sie sicher, dass der ManageEngine MIB Browser auf Ihrem System installiert ist.

4. Fügen Sie in den Eigenschaften des **SNMP Service** auf der Registerkarte **Security** zwei Communities mit den folgenden Berechtigungen hinzu:

Community	Berechtigungen
`kaspersky`	`NOTIFY`
`public`	`READ WRITE`

5. Fügen Sie im Feld **SNMP-Pakete von diesen Hosts akzeptieren** die IP-Adresse des Geräts hinzu, auf dem der ManageEngine MIB-Browser installiert ist, z. B. 10.10.10.105.

6. Geben Sie auf der Registerkarte **Traps** im Feld **Community name** `kaspersky` ein.

7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Eigenschaftenfenster des Dienstes zu schließen.

8. Laden Sie im ManageEngine MIB-Browser die Datei "adminkit.mib" aus dem Installationsordner von Kaspersky Security Center. Standardmäßig befindet sich die Datei "adminkit.mib" im Ordner <Festplatte>:\Programme\Kaspersky Lab\Kaspersky Security Center\snmp.

9. Geben Sie im Feld **Host** im Fenster des ManageEngine MIB-Browser die IP-Adresse des Geräts an, auf dem der Kaspersky Security Center Administrationsserver installiert ist.

Der SNMP-Dienst ist so konfiguriert, dass er mithilfe des Simple Network Management Protocol (SNMP) Informationen vom Administrationsserver erhält.

Kennungen des SNMP-Agenten und der SNMP-Objekte

Für Kaspersky Security Center wird der SNMP-Agent als dynamische Bibliothek `klsnmpag.dll` implementiert, die vom Installationsprogramm während der Installation des Administrationsservers registriert wird. Der SNMP-Agent arbeitet innerhalb des Prozesses `snmp.exe` (dies ist ein Windows-Dienst). Drittanbieter-Anwendungen verwenden SNMP, um in Form von Zählern erfasste Statistiken über die Leistung des Administrationsservers zu empfangen.

Jeder Zähler hat eine einmalige *Objektkennung* (auch als OID bezeichnet). Eine Objektkennung ist eine Zahlenfolge, die durch Punkte getrennt ist. Die Objektkennungen des Administrationsservers beginnen mit dem Präfix 1.3.6.1.4.1.23668.1093. Die OID des Zählers ist eine Verkettung dieses Präfixes mit einem Suffix, das den Zähler beschreibt. Beispielsweise hat ein Zähler mit dem OID-Wert 1.3.6.1.4.1.23668.1093.1.1.4 ein Suffix mit dem Wert 1.1.4.

Sie können einen SNMP-Client (z. B. Zabbix) verwenden, um den Status Ihres Systems zu überwachen. Um die Informationen abzurufen, können Sie nach einem OID-Wert suchen, der den Informationen entspricht, und diesen Wert in Ihren SNMP-Client eingeben. Dann gibt Ihnen Ihr SNMP-Client einen weiteren Wert zurück, der den Status Ihres Systems kennzeichnet.

Eine Liste der Zähler und Zählertypen befindet sich in der Datei `adminkit.mib` auf dem Administrationsserver. *MIB* steht für Management Information Base. Sie können `.mib`-Dateien über das MIB Viewer-Programm importieren und analysieren, mit der die Zählerwerte angefordert und angezeigt werden.

Den Namen des Zeichenfolgenzählers aus einer Objektkennung ableiten

Um eine Objektkennung (OID) zum Übertragen von Informationen an Anwendungen von Drittanbietern zu verwenden, müssen Sie möglicherweise einen String-Zählernamen von dieser OID abrufen.

So leiten Sie einen Zeichenfolgenzähler aus eine OID ab:

1. Öffnen Sie die Datei `adminkit.mib`, die sich auf dem Administrationsserver befindet, in einem Texteditor.
2. Suchen Sie den Namespace, der den ersten Wert beschreibt (von links nach rechts).
   Beispiel: Für das OID-Suffix 1.1.4 wäre dies `"counters" (::= { kladminkit 1 })`.
3. Suchen Sie den Namespace, der den zweiten Wert beschreibt.
   Beispiel: Für das OID-Suffix 1.1.4 wäre dies `counters 1`, was für `deployment` steht.
4. Suchen Sie den Namespace, der den dritten Wert beschreibt.
   Beispiel: Für das OID-Suffix 1.1.4 wäre dies `deployment 4`, was für `hostsWithAntivirus`.

Der Name des Zeichenfolgenzählers setzt sich beispielhaft aus der Verkettung dieser Werte zusammen: `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, und entspricht der OID mit dem Wert 1.3.6.1.4.1.23668.1093.1.1.4.

Werte von Objektkennungen für SNMP

In der folgenden Tabelle sind die Werte und Beschreibungen der Objektkennungen (auch als OIDs bezeichnet) aufgeführt, die zum Übertragen von Informationen über die Leistung des Administrationsservers an Drittanbieter-Anwendungen verwendet werden.

Werte und Beschreibungen von Objektkennungen für SNMP

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Bereitstellungsstatus. Es gibt folgende Statusvarianten: • **Information**. Die Lizenz gilt nicht mehr für n Geräte. • **Warnung**. Eine der folgenden Varianten: Es gibt Geräte mit installierten Kaspersky-Anwendungen auf insgesamt n Geräten in den Administrationsserver-Gruppen (n > m). Lizenz L läuft auf n Geräten in m Tagen ab. Aufgabe T für die Installation von Anwendungen wurde auf n Geräten erfolgreich abgeschlossen. Für m Geräte ist ein Neustart erforderlich. • **Kritisch**. Die Lizenz ist für n Geräte abgelaufen. • **OK**. Keine der oben genannten Varianten.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	`deploymentStatus` gibt an, dass die Administrationsserver-Gruppe zu viele Geräte ohne verwaltete Anwendungen enthält. Der Wert ist 1, wenn einige Geräte ohne verwaltete Anwendungen gefunden wurden. Andernfalls ist der Wert 0.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	`deploymentStatus` gibt an, dass die Aufgabe zur Remote-Installation auf einigen Geräten fehlgeschlagen ist. Die Anzahl dieser Geräte kann mit `hostsRemoteInstallFailed` abgerufen werden.
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	`deploymentStatus` gibt an, dass Geräte existieren, auf denen die Lizenz innerhalb den nächsten 7 Tagen abläuft. Die Anzahl dieser Geräte kann mit `hostsLicenseExpiring` abgerufen werden.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	`deploymentStatus` gibt an, dass es Geräte mit einer abgelaufenen Lizenz gibt. Die Anzahl dieser Geräte können Sie mit `hostsLicenseExpired` abrufen.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Anzahl der Geräte in den Administrationsserver-Gruppen
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Anzahl der Geräte mit installierten verwalteten Programmen in den Administrationsserver-Gruppen.
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Anzahl der Geräte, auf denen die Aufgabe zur Remote-Installation fehlgeschlagen ist.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	ID eines Lizenzschlüssels, der in weniger als 7 Tagen abläuft.
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	ID des abgelaufenen Lizenzschlüssels.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Anzahl der Tage bis zum Ablauf der Lizenz. Für diesen Parameter gilt der Lizenzzeitraum als abgelaufen, wenn bis zum Ablaufdatum weniger als 7 Tage verbleiben. Wenn bis zum Ablaufdatum mehr als 7 Tage verbleiben, ist der Wert des Parameters "0".
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Anzahl der Geräte mit einer Lizenz, die in weniger als 7 Tagen abläuft.
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Anzahl der Geräte mit einer abgelaufenen Lizenz.

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
`updatesStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.2.1	Aktueller Status des Updates der Antiviren-Datenbanken. Es gibt folgende Statusvarianten: • **Information**. Die Antiviren-Datenbanken auf dem Administrationsserver oder auf den Geräten wurden seit mehr als 1 Tag nicht aktualisiert und Programm wurde vor weniger als 1 Tag installiert. • **Warnung**. Die Antiviren-Datenbanken auf dem Administrationsserver oder auf den Geräten wurden seit mehr als 3 Tagen nicht aktualisiert. Dieser Wert kann in den Gruppeneinstellungen geändert werden. • **Kritisch**. Die Antiviren-Datenbanken auf dem Administrationsserver oder auf den Geräten wurden seit mehr als 7 Tagen nicht aktualisiert. Dieser Wert kann in den Gruppeneinstellungen geändert werden. • **OK**. Keine der oben genannten Varianten.
`serverNotUpdated`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.1	Das letzte Update des Administrationsservers liegt lange zurück. Die als "lang" angesehene Zeit wird in `updatesStatus` festgelegt.
`notUpdatedHosts`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.2	Einige Geräte wurden über längere Zeit nicht aktualisiert (standardmäßig nach 3 Tagen **Warnung** und nach 7 Tagen **Kritisch**). Die Anzahl dieser Geräte können Sie mit `hostsNotUpdated` abrufen.
`lastServerUpdateTime`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.2.3	Letzter Zeitpunkt der Aktualisierung der Antiviren-Datenbanken auf dem Administrationsserver.
`hostsNotUpdated`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.2.4	Anzahl der Geräte, deren Antiviren-Datenbanken für längere Zeit nicht aktualisiert wurden (standardmäßig nach 3 Tagen **Warnung** und nach 7 Tagen **Kritisch**). Sollten Geräte den Update-Status **Kritisch** besitzen, werden nur diese Geräte gezählt. Den Update-Status können Sie mittels `updatesStatus` abrufen.
`protectionStatus`	`INTEGER { ok(0), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.3.1	Status des Echtzeitschutzes. Eine der folgenden Varianten: • **Warnung**. Eine der folgenden Varianten: Auf einem Gerät, das zur Administrationsserver-Gruppe gehört, wird eine Sicherheitsverletzung festgestellt. Aufgrund von Verschlüsselungsfehlern wurde für einige Geräte der Schutzstatus geändert. Die letzte vollständige Untersuchung liegt lange zurück. • **Kritisch**. Der Antiviren-Schutz funktioniert auf einigen Geräten in den Administrationsserver-Gruppen nicht. • **OK**. Keine der oben genannten Varianten.
`antivirusNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.1	Auf einigen Geräten wird keine Sicherheitsanwendung ausgeführt. Die Anzahl dieser Geräte können Sie mit `hostsAntivirusNotRunning` abrufen.
`realtimeNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.2	Auf einigen Geräten wird der Echtzeitschutz nicht ausgeführt. Die Anzahl dieser Geräte können Sie mit `hostsRealtimeNotRunning` abrufen.
`psRealtimeLevelChanged`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.2.3	Die Anzahl der Geräte, deren Stufe des Echtzeitschutzes von der vom Administrator festgelegten Stufe abweicht
`notCuredFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.4	Es gibt Geräte, die nicht desinfizierte Objekte enthalten. Die Anzahl dieser Geräte können Sie mit `hostsNotCuredObject` abrufen.
`tooManyThreats`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.5	Auf einigen Geräten wurden Bedrohungen gefunden. Die Anzahl dieser Geräte können Sie mit `hostsTooManyThreats` abrufen.

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Der Status des Virenangriffs auf dem System. Der Wert ist gleich 1, wenn während einer bestimmten Zeit eine bestimmte Anzahl von Viren gefunden wurde, andernfalls 0. Die Anzahl der Viren und die Zeitdauer werden auf dem Administrationsserver mithilfe der Einstellungen für `Virenangriffe` angegeben.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Es wurden Schwachstellen gefunden.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Es wurden Fehler bei der Verschlüsselung erkannt, die den Schutzstatus des Geräts geändert haben.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	Auf einigen Geräten wurden Schwachstellen gefunden.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Es wurden Geräte gefunden, für die längere Zeit keine vollständige Untersuchung durchgeführt wurde.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Es wurden Geräte gefunden, auf denen der Administrationsagent erst nach einem Neustart ausgeführt wird.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Anzahl der Geräte, auf denen keine Sicherheitsanwendungen ausgeführt werden.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Anzahl der Geräte, auf denen der Echtzeitschutz die nicht ausgeführt wird.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Anzahl der Geräte mit einer inakzeptablen Stufe des Echtzeitschutzes.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Anzahl der Geräte, die nicht desinfizierte Objekte enthalten.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Anzahl der Geräte, die Bedrohungen enthalten.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Der Status der vollständigen Untersuchung auf Viren ist einer der folgenden: • **Information**. Seit der Installation des Programms sind weniger als 7 Tage vergangen. • **Warnung**. Nach der Programminstallation wurde länger als 7 Tage keine vollständige Untersuchung auf Viren durchgeführt. • **Kritisch**. Nach der Programminstallation wurde länger als 14 Tage keine vollständige Untersuchung auf Viren durchgeführt. • **OK**. Keine der oben genannten Varianten.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Einige Geräte wurden seit einer gewissen Zeit nicht untersucht. Die Anzahl dieser Geräte können Sie mit `hostsNotScannedLately` abrufen. Die Zeitdauer wird in `fullScanStatus` angegeben.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Anzahl der Geräte, die in einem bestimmten Zeitraum nicht untersucht wurden. Die Zeitdauer wird in `fullScanStatus` angegeben.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Status des logischen Netzwerks des Administrationsservers. Eine der folgenden Varianten: • **Warnung**. Wenn Geräte, auf die kein Zugriff besteht, einen Status des Typs "Warnung" besitzen, oder wenn Geräte existieren, die keiner Administrationsserver-Gruppe angehören. • **Kritisch**. Wenn es Geräte gibt, deren Kontrolle der Administrationsserver verloren hat, oder wenn es Geräte mit einem kritischen Status gibt und auf die nicht zugegriffen werden kann. • **OK**. Keine der oben genannten Varianten.

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Einige Geräte waren längere Zeit nicht mit dem Administrationsserver verbunden (7 Tage oder länger für ein Gerät mit dem Status **Warnung** und 4 Tage für ein Gerät mit dem Status **Kritisch**). Die Anzahl dieser Geräte können Sie mit hostsNotConnectedLongTime abrufen.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Es gibt Geräte, die nicht mehr vom Administrationsserver kontrolliert werden. Die Anzahl dieser Geräte können Sie mit hostsControlLost abrufen.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Anzahl der vom Administrationsserver gefundenen Geräte, die keiner Administrationsserver-Gruppe angehören.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Anzahl der Gruppen des Administrationsservers.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Anzahl der Geräte, die längere Zeit nicht mit dem Administrationsserver verbunden waren. Die als "lang" angesehene Zeit wird in notConnectedLongTime festgelegt.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Anzahl der Geräte, die nicht vom Administrationsserver kontrolliert werden.
eventsStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.6.1	Status des Ereignis-Subsystems ist einer der folgenden: • **Warnung**. Eine der folgenden Varianten: Geräte Administrationsserver-Gruppe haben lange nicht mehr nach Windows-Updates gesucht. Es gibt Geräte mit Statusproblemen. • **Kritisch**. Eine der folgenden Varianten: Auf mindestens einem Gerät liegt ein Ereignis mit der Priorität "Kritisch" vor. Auf mindestens einem Gerät liegt ein Ereignis mit der Priorität "Error" vor. Es gibt ein Ereignis, das besagt, dass eine Aufgabe auf mindestens einem Gerät nicht erfolgreich abgeschlossen wurde. Geräte Administrationsserver-Gruppe haben lange nicht mehr nach Windows-Updates gesucht. Es gibt Geräte mit Statusproblemen. • **Information.** Eine der folgenden Varianten: Alle Geräte wurden vor weniger als einer Woche vollständig auf Viren untersucht. Die Remote-Installationsaufgaben sind abgeschlossen und kein Gerät muss neu gestartet werden. Das letzte Update des Administrationsservers liegt weniger als eine Woche zurück. Der Administrationsserver erhielt lange keine Updates, wird aber gerade aktualisiert. • **OK**. Keine der oben genannten Varianten.
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	eventsStatus zeigt, dass auf dem Administrationsserver einige kritische Ereignisse vorliegen. Die Anzahl dieser Ereignisse können Sie mit criticalEventsCount abrufen. Der Wert ist gleich 1, wenn auf einem beliebigen Gerät mindestens ein kritisches Ereignis vorliegt, andernfalls ist der Wert 0.
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	Anzahl der kritischen Ereignisse auf dem Administrationsserver.

Problemlösung

In diesem Abschnitt werden Lösungen für einige typische Probleme aufgeführt, die bei der Verwendung des SNMP-Dienstes auftreten können.

Drittanbieter-Programme können keine Verbindung zum SNMP-Dienst herstellen

Stellen Sie sicher, dass der SNMP-Dienst installiert und konfiguriert ist, wie im Abschnitt Den SNMP-Dienst für die Verwendung mit Kaspersky Security Center konfigurieren beschrieben.

Der SNMP-Dienst funktioniert, das Drittanbieterprogramm kann jedoch keine Werte abrufen

Ermöglichen Sie die Ablaufverfolgung von SNMP-Agenten und stellen Sie sicher, dass eine nicht leere Datei erstellt wird. Dies bedeutet, dass der SNMP-Agent ordnungsgemäß registriert ist und funktioniert. Lassen Sie danach in den Nebendiensteinstellungen Verbindungen vom SNMP-Dienst zu. Wenn ein Nebendienst auf demselben Host wie der SNMP-Agent ausgeführt wird, sollte die Liste der IP-Adressen entweder die IP-Adresse dieses Hosts oder `loopback 127.0.0.1` enthalten.

Ein SNMP-Dienst, der mit Agenten kommuniziert, sollte unter Windows ausgeführt werden. Sie können die Pfade zu SNMP-Agenten in der Windows-Registrierung über regedit angeben.

- Microsoft Windows 10:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Für Windows Vista und Windows Server 2008:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Sie können die Ablaufverfolgung von SNMP-Agenten auch über regedit zulassen.

- Für 32-Bit-Systeme:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- Für 64-Bit-Systeme:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

Die Werte stimmen nicht mit dem Status der Verwaltungskonsole überein

Um die Belastung des Administrationsservers zu verringern, wird das Zwischenspeichern von Werten für den SNMP-Agenten implementiert. Die Latenz zwischen dem aktualisierten Cache und den auf dem Administrationsserver geänderten Werten kann zu Fehlanpassungen zwischen den vom SNMP-Agenten zurückgegebenen und den tatsächlichen Werten führen. Wenn Sie mit Programmen von Drittanbietern arbeiten, sollten Sie diese mögliche Latenz berücksichtigen.

Arbeiten in einer Cloud-Umgebung

Dieser Abschnitt enthält Informationen über die Bereitstellung und Wartung von Kaspersky Security Center in Cloud-Umgebungen wie Amazon Web Services, Microsoft Azure oder Google Cloud.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Über die Arbeit in der Cloud-Umgebung

Kaspersky Security Center 15.1 arbeitet nicht nur mit Geräten vor Ort, sondern stellt auch spezielle Funktionen zum Arbeiten in einer Cloud-Umgebung bereit. Kaspersky Security Center arbeitet mit folgenden virtuellen Maschinen:

- Amazon EC2-Instances (im Folgenden auch als *Instances* bezeichnet). Eine Amazon EC2-Instance ist eine virtuelle Maschine, die auf der Grundlage der Amazon Web Services-Plattform (AWS) erstellt wird. Kaspersky Security Center verwendet die AWS-*API* (Application Programming Interface).
- Virtuelle Maschinen in Microsoft Azure. Kaspersky Security Center verwendet die Azure-API.
- Instanzen virtueller Maschinen in Google Cloud. Kaspersky Security Center verwendet die Google-API.

Sie können Kaspersky Security Center auf einer Instance oder einer virtuellen Maschine bereitstellen, um den Schutz von Geräten in einer Cloud-Umgebung zu verwalten und die besonderen Funktionen von Kaspersky Security Center für die Arbeit in der Cloud-Umgebung zu nutzen. Zu diesen Funktionen gehören:

- Verwenden von API-Instrumenten, um Geräte abzufragen, die sich in der Cloud-Umgebung befinden
- Verwenden von API-Instrumenten zur Installation des Administrationsagenten und der Sicherheitsanwendungen auf Geräten in einer Cloud-Umgebung
- Suche nach Geräten anhand dem Merkmal der Zugehörigkeit zu einem bestimmten Cloud-Segment

Sie können auch eine Instance oder eine virtuelle Maschine, auf der sich ein Kaspersky Security Center Administrationsserver befindet, für den Schutz von Geräten vor Ort verwenden (z. B., wenn es sich für Sie herausstellt, dass ein Cloud-Server vorteilhafter in der Bedienung und Pflege ist, als ein physischer). In diesem Fall wird die Arbeit mit dem Administrationsserver genauso konfiguriert wie wenn der Administrationsserver auf einem Gerät vor Ort installiert wäre.

Wenn Kaspersky Security Center von einem zahlungspflichtigen Amazon Machine Image (AMI) (in AWS) oder einem nutzungsbasierten, monatlich verrechneten SKU (in Azure) verteilt wurde, wird "Schwachstellen- und Patch-Management" (einschließlich der Integration in SIEM-Systeme) automatisch aktiviert, während die Komponente "Mobile Geräte verwalten" nicht verwendet werden kann.

Der Administrationsserver wird zusammen mit der Verwaltungskonsole installiert. Kaspersky Security für Windows Server wird ebenfalls automatisch auf dem Gerät installiert, auf dem der Administrationsserver installiert ist.

Sie können Kaspersky Security Center mit dem Assistenten zum Konfigurieren der Cloud-Umgebung unter Berücksichtigung der Besonderheiten bei der Arbeit in einer Cloud-Umgebung konfigurieren.

Szenario: Bereitstellung für eine Cloud-Umgebung

In diesem Abschnitt wird die Vorgehensweise zur Bereitstellung von Kaspersky Security Center für die Arbeit in Cloud-Umgebungen wie Amazon Web Services, Microsoft Azure und Google Cloud beschrieben.

Nach Abschluss des Verteilungsszenarios werden der Kaspersky Security Center Administrationsserver und die Verwaltungskonsole gestartet und mit den Standardeinstellungen konfiguriert. Auf den ausgewählten Amazon EC2-Instanzen oder Microsoft Azure virtuellen Maschinen wird der Antiviren-Schutz unter der Verwaltung von Kaspersky Security Center verteilt. Im Folgenden können Sie Kaspersky Security Center weiter anpassen, die komplizierte Struktur der Administrationsgruppen erstellen, verschiedene Richtlinien und Aufgaben, für die Gruppen erstellen.

Die Bereitstellung von Kaspersky Security Center zur Arbeit in der Cloud-Umgebung besteht aus folgenden Schritten:

1. Vorbereitende Maßnahmen
2. Bereitstellung eines Administrationsservers
3. Installation der Antiviren-Programme von Kaspersky auf zu schützenden virtuellen Geräten
4. Konfiguration der Einstellungen für Update-Download
5. Anpassen der Einstellungen für die Arbeit mit den Berichten über den Schutzstatus der Geräte

Für die Durchführung der Erstkonfiguration ist der Assistent zur Konfiguration der Cloud-Umgebung vorgesehen. Er startet das erste Mal automatisch, wenn Kaspersky Security Center von einem einsatzbereiten Image installiert wird. Sie können den Assistenten jederzeit manuell ausführen. Außerdem können Sie alle Aktionen, welche er ausführt, auch manuell ausführen.

Es wird empfohlen, mindestens eine Stunde für die Bereitstellung des Kaspersky Security Center Administrationsservers in der Cloud-Umgebung und mindestens einen Werktag für die Bereitstellung des Schutzes in der Cloud-Umgebung einzuplanen.

Die Bereitstellung von Kaspersky Security Center in der Cloud-Umgebung erfolgt in mehreren Schritten:

1. **Planung der Konfiguration der Cloud-Segmente**

   Erfahren Sie, wie Kaspersky Security Center in einer Cloud-Umgebung funktioniert. Planen Sie, wo sich der Administrationsserver befinden soll (innerhalb oder außerhalb der Cloud-Umgebung) und bestimmen Sie, wie viele Cloud-Segmente Sie schützen möchten. Wenn Sie planen, den Administrationsserver außerhalb der Cloud-Umgebung zu platzieren, oder wenn Sie vorhaben, mehr als 5000 Geräte zu schützen, müssen Sie den Administrationsserver manuell installieren.

   Um mit Google Cloud zu arbeiten, können Sie den Administrationsserver nur manuell installieren.

2. **Planung der Ressourcen**

   Stellen Sie sicher, dass Sie alle nötigen Voraussetzungen für die Bereitstellung erfüllen.

3. **Abonnement für Kaspersky Security Center in Form eines einsatzbereiten Images**

Wählen Sie eines der einsatzbereiten AMIs im Shop AWS Marketplace aus oder wählen Sie ein nutzungsbasiertes, monatlich verrechnetes SKU im Azure Marketplace, bezahlen Sie es erforderlichenfalls gemäß den Marketplace-Regeln (oder verwenden Sie das BYOL-Modell) und verwenden Sie anschließend dieses Image zur Bereitstellung der Amazon EC2-Instanz oder der virtuellen Maschine von Microsoft Azure mit installiertem Kaspersky Security Center.

Dieser Schritt ist nur erforderlich, wenn Sie planen, den Administrationsserver auf einer Instanz oder einer virtuellen Maschine innerhalb der Cloud-Umgebung zu verteilen, und dabei maximal 5.000 Geräte schützen möchten. Andernfalls ist dieser Schritt nicht erforderlich. Stattdessen müssen Sie den Administrationsserver, die Verwaltungskonsole und das DBMS manuell installieren.

Dieser Schritt ist für Google Cloud nicht verfügbar.

4. **Speicherort des DBMS bestimmen**

   Bestimmen Sie, wo sich Ihr DBMS befinden soll.

   Wenn Sie planen, eine Datenbank außerhalb der Cloud-Umgebung zu verwenden, stellen Sie sicher, dass Sie eine funktionierende Datenbank haben.

   Wenn Sie planen, Amazon Relational Database Service (RDS) zu verwenden, erstellen Sie in der AWS Cloud-Umgebung eine Datenbank mit RDS.

   Wenn Sie planen, Microsoft Azure SQL DBMS zu verwenden, erstellen Sie in der Microsoft Azure Cloud-Umgebung eine Datenbank mit dem Azure Database-Dienst.

   Wenn Sie planen, Google MySQL zu verwenden, erstellen Sie eine Datenbank in Google Cloud (Weitere Informationen entnehmen Sie bitte https://cloud.google.com/sql/docs/mysql).

5. **Manuelle Installation des Administrationsservers und der Verwaltungskonsole (basierend auf Microsoft Management Console und/oder der web-basierten Konsole) auf ausgewählten Geräten**

   Installieren Sie den Administrationsserver, die Verwaltungskonsole und das DBMS auf den ausgewählten Geräten wie in dem Hauptinstallationsszenario von Kaspersky Security Center beschrieben.

   Dieser Schritt ist erforderlich, wenn Sie planen, den Administrationsserver außerhalb der Cloud-Umgebung zu platzieren, oder wenn Sie mehr als 5000 Geräte schützen möchten. Stellen Sie anschließen sicher, dass Ihr Administrationsserver die Hardwarevoraussetzungen erfüllt. Andernfalls ist dieser Schritt nicht erforderlich und ein Abonnement für Kaspersky Security Center in Form eines einsatzbereiten Images aus AWS Marketplace, Azure Marketplace oder Google Cloud ist in diesem Fall ausreichend.

6. **Sicherstellen, dass ein Administrationsserver die Berechtigungen zur Arbeit mit Cloud-APIs besitzt**

   Wechseln Sie in AWS zu der AWS-Managementkonsole und erstellen Sie eine IAM-Rolle oder ein IAM-Benutzerkonto. Die erstellte IAM-Rolle (bzw. das IAM-Benutzerkonto) erlaubt es Kaspersky Security Center mit der AWS API zu arbeiten: Cloud-Segmente abfragen und den Schutz bereitstellen.

   Erstellen Sie in Azure ein Abonnement und eine Anwendungs-ID samt Kennwort. Kaspersky Security Center verwendet diese Anmeldedaten bei der Interaktion mit der Azure-API zur Abfrage von Cloud-Segmenten und der Bereitstellung des Schutzes.

   Registrieren Sie ein Projekt und erhalten Sie Ihre Projekt-ID und einen privaten Schlüssel in Google Cloud. Kaspersky Security Center verwendet diese Anmeldeinformationen, um Cloud-Segmente mithilfe der Google-API abzufragen.

7. **Erstellen einer IAM-Rolle für geschützte Instanzen (nur für AWS)**

   Erstellen Sie in der AWS-Managementkonsole eine IAM-Rolle, die den Satz der Berechtigungen für das Ausführen von Abfragen von AWS bestimmt. Die erstellte Rolle weisen Sie in der Folge neuen Instanzen zu. Die IAM-Rolle wird für die Installation von Programmen auf Instanzen mithilfe von Kaspersky Security Center benötigt.

8. **Vorbereitung einer Datenbank mithilfe von Amazon Relational Database Service oder Microsoft Azure SQL**

Wenn Sie planen, Amazon Relational Database Service (RDS) zu verwenden, erstellen Sie eine Amazon RDS-DB-Instance und einen S3-Bucket, auf dem das Datenbank-Backup gesichert wird. Sie können diesen Schritt überspringen, wenn Sie eine Datenbank auf derselben EC2-Instanz betreiben möchten, auf welcher der Administrationsserver installiert ist, oder wenn Sie möchten, dass sich Ihre Datenbank an einem anderen Ort befindet.

Wenn Sie planen, Microsoft Azure SQL zu verwenden, erstellen Sie ein Speicherkonto und eine Datenbank in Microsoft Azure.

Wenn Sie planen, Google MySQL zu verwenden, konfigurieren Sie eine Datenbank in Google Cloud (Weitere Informationen entnehmen Sie bitte https://cloud.google.com/sql/docs/mysql).

9 Lizenzierung von Kaspersky Security Center für die Arbeit in der Cloud-Umgebung

Stellen Sie sicher, dass Sie Kaspersky Security Center zur Arbeit in der Cloud-Umgebung lizenziert haben, und stellen Sie den Aktivierungscode oder die Schlüsseldatei bereit, damit das Programm diese zum Lizenzspeicher hinzufügt. Diese Phase kann während der Konfiguration der Cloud-Umgebung abgeschlossen werden.

Diese Etappe ist obligatorisch, wenn Kaspersky Security Center aus einem kostenlosen einsatzbereiten AMI auf Basis des BYOL-Modells installiert wurde, oder wenn Sie Kaspersky Security Center manuell ohne die Verwendung von AMIs installieren. In jedem dieser Fälle benötigen Sie zur Aktivierung von Kaspersky Security Center eine Lizenz für Kaspersky Security for Virtualization oder für Kaspersky Hybrid Cloud Security.

Wenn Sie ein Kaspersky Security Center verwenden, das aus einem einsatzbereiten Image installiert wurde, ist dieser Schritt nicht erforderlich und das entsprechende Fenster des Assistenten zur Konfiguration der Cloud-Umgebung wird nicht angezeigt.

10 Autorisieren in der Cloud-Umgebung

Stellen Sie Kaspersky Security Center Ihre AWS-, Azure- oder Google Cloud-Anmeldedaten bereit, damit Kaspersky Security Center über die erforderlichen Berechtigungen verfügt. Diese Phase kann während der Autorisierung in der Cloud-Umgebung abgeschlossen werden.

11 Abfragen eines Cloud-Segments, damit der Administrationsserver Informationen über die Geräte im Cloud-Segment empfangen kann

Starten Sie die Abfrage von Cloud-Segmenten. In der AWS-Umgebung empfängt Kaspersky Security Center Adressen und Namen aller Instanzen, für die der Zugriff durch die Berechtigungen der IAM-Rolle (bzw. die Berechtigungen des IAM-Benutzers) geregelt ist. In der Microsoft Azure-Umgebung empfängt Kaspersky Security Center Adressen und Namen aller virtuellen Maschinen, für die der Zugriff durch die Berechtigungen der Rolle "Reader" geregelt ist.

Im Folgenden können Sie mithilfe von Kaspersky Security Center die Anwendungen von Kaspersky und von anderen Herstellern auf den gefundenen Instanzen bzw. virtuellen Maschinen installieren.

Da Kaspersky Security Center die Abfrage regelmäßig startet, werden neue Instanzen oder virtuelle Maschinen automatisch gefunden.

12 Zusammenfassung aller Geräte des Netzwerkes in der Administrationsgruppe Cloud

Verschieben Sie alle gefundenen Instanzen oder virtuellen Maschinen in die Administrationsgruppe **Verwaltete Geräte\Cloud**, damit sie für die zentralisierte Verwaltung verfügbar werden. Wenn Sie die Geräte auf Untergruppen aufteilen, beispielsweise nach installiertem Betriebssystem, können Sie innerhalb der Gruppe **Verwaltete Geräte \ Cloud** mehrere Administrationsgruppen erstellen. Sie können das automatische Verschieben aller Geräte, die während der regelmäßigen Abfragen gefunden werden, in die Gruppe **Verwaltete Geräte\Cloud** aktivieren.

13. **Verbindung der Netzwerkgeräte mit dem Administrationsserver mithilfe des Administrationsagenten**

    Installieren Sie den Administrationsagenten auf Geräten in der Cloud-Umgebung. Der Administrationsagent ist eine Komponente von Kaspersky Security Center, die für die Kommunikation der Geräte mit dem Administrationsserver zuständig ist. Die Einstellungen des Administrationsagenten werden standardmäßig automatisch angepasst.

    Sie können den Administrationsagenten auf jedem Gerät lokal installieren. Sie können den Administrationsagenten mithilfe von Kaspersky Security Center auch per Remote-Zugriff auf den Geräten installieren. Alternativ können Sie diesen Schritt auch überspringen und den Administrationsagenten zusammen mit den aktuellen Versionen der Sicherheitsanwendung installieren.

14. **Installation der aktuellen Versionen der Sicherheitsanwendung auf den Geräten im Netzwerk**

    Wählen Sie die Geräte aus, auf denen Sie die Sicherheitsanwendungen installieren möchten, und installieren Sie anschließend die aktuellen Versionen der Sicherheitsanwendungen auf diesen Geräten. Sie können die Installation entweder remote mithilfe von Kaspersky Security Center auf einem Administrationsserver oder lokal durchführen.

    Möglicherweise müssen Sie die Installationspakete für diese Programme manuell erstellen.

    Für Instanzen und virtuelle Maschinen unter Linux ist das Programm Kaspersky Endpoint Security für Linux vorgesehen.

    Für Instanzen und virtuelle Maschinen unter Windows ist das Programm Kaspersky Security für Windows Server vorgesehen.

15. **Konfiguration der Update-Einstellungen**

Die Aufgabe **Suche nach Schwachstellen und erforderlichen Updates** wird während des Starts der Konfiguration der Cloud-Umgebung automatisch erstellt. Sie können sie auch manuell erstellen. Diese Aufgabe gewährleistet die automatische Suche und den Download der notwendigen Programm-Updates für die folgende Installation auf den Geräten im Netzwerk mithilfe von Kaspersky Security Center.

Es wird empfohlen, nach Beendigung der Konfiguration der Cloud-Umgebung den folgenden Schritt abzuschließen:

1. **Konfiguration der Berichte**

    Sie können die Berichte auf der Registerkarte **Überwachung** im Arbeitsbereich des Knotens **Administrationsserver** anzeigen. Sie können Berichte auch per E-Mail erhalten. Die Berichte auf der Registerkarte **Überwachung** sind standardmäßig verfügbar. Um den Empfang von Berichten per E-Mail anzupassen, geben Sie die E-Mail-Adressen ein, an welche die Berichte gesendet werden sollen, und passen Sie anschließend das Format der Berichte an.

Ergebnisse

Nach Abschluss dieses Szenarios können Sie sicherstellen, dass die Erstkonfiguration erfolgreich war:

- Sie müssen dazu in der Lage sein, eine Verbindung zum Administrationsserver via Verwaltungskonsole oder Kaspersky Security Center Web Console herzustellen.
- Die aktuellsten Versionen der Sicherheitsanwendungen von Kaspersky müssen auf den verwalteten Geräten installiert sein und ausgeführt werden.
- Kaspersky Security Center muss die Standardrichtlinien und Aufgaben für alle verwalteten Geräte erstellt haben.

Voraussetzungen für die Softwareverteilung von Kaspersky Security Center in einer Cloud-Umgebung

Bevor Sie mit der Bereitstellung von Kaspersky Security Center in einer Cloud-Umgebung von Amazon Web Services oder Microsoft Azure beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen gegeben sind:

- Internetzugang
- Eines der folgenden Konten:
  - Amazon Web Services-Konto (für das Arbeiten mit AWS)
  - Microsoft-Konto (für das Arbeiten mit Azure)
  - Google-Konto (für das Arbeiten mit Google Cloud)
- Eine der folgenden Varianten:
  - Lizenz für Kaspersky Security for Virtualization
  - Lizenz für Kaspersky Hybrid Cloud Security
  - Mittel zum Erwerb einer solchen Lizenz (Kaspersky Security for Virtualization oder Kaspersky Hybrid Cloud Security)
  - Mittel zum Bezahlen eines gebrauchsfertigen Images bei Azure Marketplace
- Handbücher für die aktuellen Versionen von Kaspersky Endpoint Security für Linux und Kaspersky Security für Windows Server

Hardwarevoraussetzungen des Administrationsservers in einer Cloud-Umgebung

Für die Bereitstellung in Cloud-Umgebungen entsprechen die Anforderungen an den Administrationsserver und den Datenbankserver den gleichen Anforderungen, wie an einen physischen Administrationsserver (in Abhängigkeit davon, wie viele Geräte Sie verwalten wollen). Einzelheiten entnehmen Sie bitte der Dokumentation zur Cloud-Umgebung.

Varianten der Lizenzierung in der Cloud-Umgebung

Die Arbeit in der Cloud-Umgebung gehört nicht zu den Grundfunktionen von Kaspersky Security Center und erfordert deshalb eine Lizenz.

Für die Arbeit in der Cloud-Umgebung stehen zwei Varianten der Lizenzierung von Kaspersky Security Center zur Verfügung:

- Zahlungspflichtiges AMI (in Amazon Web Services) oder nutzungsbasiertes, monatlich verrechnetes SKU (in Microsoft Azure).

  Das gewährt eine Lizenz für Kaspersky Security Center sowie Lizenzen für Kaspersky Endpoint Security für Linux und Kaspersky Security für Windows Server. Sie müssen gemäß den Vorgaben der von Ihnen verwendeten Cloud-Umgebung bezahlen.

  Dieses Modell erlaubt maximal 200 Client-Geräte pro Administrationsserver.

- Gebrauchsfertiges, kostenloses Image mit Nutzung einer proprietären Lizenz entsprechend dem BYOL-Modell (Bring Your Own License).

  Für die Lizenzierung von Kaspersky Security Center in AWS oder Azure ist eine Lizenz für eines der folgenden Programme erforderlich:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  Das BYOL-Modell lässt bis zu 100.000 Client-Geräte pro Administrationsserver zu. Mit diesem Modell können Sie außerdem Geräte außerhalb der Cloud-Umgebungen von AWS, Azure oder Google verwalten.

  Das BYOL-Modell kann für jeden der folgenden Fälle gewählt werden:

  - Sie besitzen bereits eine gültige Lizenz für Kaspersky Security for Virtualization.
  - Sie besitzen bereits eine gültige Lizenz für Kaspersky Hybrid Cloud Security.
  - Sie sind bereit, unmittelbar vor der Bereitstellung von Kaspersky Security Center eine Lizenz zu erwerben.

  Bei der Erstkonfiguration fragt Kaspersky Security Center nach dem Aktivierungscode bzw. der Schlüsseldatei.

  Bei der Auswahl von BYOL müssen Sie für die Nutzung von Kaspersky Security Center über Azure Marketplace oder AWS Marketplace nichts bezahlen.

In beiden Fällen wird Schwachstellen- und Patch-Management automatisch aktiviert, während die Komponente "Mobile Geräte verwalten" nicht aktiviert werden kann.

Wenn beim Aktivieren der Funktion "Arbeit in der Cloud-Umgebung" mittels Lizenz für Kaspersky Hybrid Cloud Security ein Fehler auftritt, verwenden Sie die Schlüsseldatei.

Nach dem Erwerb eines Abonnements von Kaspersky Security Center erhalten Sie eine Amazon EC2-Instance (Amazon Elastic Compute Cloud) oder eine Microsoft Azure virtuelle Maschine mit dem Kaspersky Security Center Administrationsserver. Die Installationspakete für Kaspersky Security für Windows Server und Kaspersky Endpoint Security für Linux stehen auf dem Administrationsserver zur Verfügung. Diese Anwendungen können auf den Geräten in der Cloud-Umgebung installiert werden. Die Anwendungen benötigen keine Lizenzierung.

Wenn ein verwaltetes Gerät für den Administrationsserver länger als eine Woche nicht sichtbar ist, wechselt die Anwendung (Kaspersky Security für Windows Server oder Kaspersky Endpoint Security für Linux) auf diesem Gerät in den eingeschränkten Funktionsmodus. Um die Anwendung wieder zu aktivieren, müssen Sie das Gerät, auf dem die Anwendung installiert ist, wieder sichtbar für den Administrationsserver machen.

Datenbankoptionen zum Arbeiten in einer Cloud-Umgebung

Sie müssen über eine Datenbank verfügen, um mit Kaspersky Security Center arbeiten zu können. Beim Bereitstellen von Kaspersky Security Center in AWS, Microsoft Azure oder Google Cloud, haben Sie drei Optionen:

- Erstellen Sie eine lokale Datenbank auf demselben Gerät mit dem Administrationsserver. Kaspersky Security Center wird mit einer SQL Server Express-Datenbank ausgeliefert, die bis zu 5.000 verwaltete Geräte unterstützt. Wählen Sie diese Option, wenn SQL Server Express Edition für Ihre Bedürfnisse ausreichend ist.

- Erstellen Sie eine Datenbank mit dem Relational Database Service (RDS) in der AWS Cloud-Umgebung oder mit dem Azure Datenbankdienst in der Microsoft Azure Cloud-Umgebung. Wählen Sie diese Option, wenn Sie ein anderes DBMS als SQL Express verwenden möchten. Ihre Daten werden in die Cloud-Umgebung übertragen, wo sie verbleiben, und Sie haben keine zusätzlichen Ausgaben. Wenn Sie bereits mit Kaspersky Security Center vor Ort arbeiten und Daten in Ihrer Datenbank haben, können Sie Ihre Daten in die neue Datenbank übertragen.

  Für die Arbeit in Google Cloud Platform können Sie nur Cloud SQL für MySQL verwenden.

- Verwenden Sie einen vorhandenen Datenbankserver. Wählen Sie diese Option, wenn Sie bereits über einen Datenbankserver verfügen und diesen für Kaspersky Security Center verwenden möchten. Wenn sich dieser Server außerhalb der Cloud-Umgebung befindet, werden Ihre Daten über das Internet übertragen, was zu Zusatzkosten führen kann.

Der Vorgang zur Bereitstellung von Kaspersky Security Center in der Cloud-Umgebung verfügt über einen speziellen Schritt zum Erstellen (Auswählen) einer Datenbank.

Arbeit mit der Cloud-Umgebung Amazon Web Services

In diesem Abschnitt erfahren Sie, wie Sie sich für die Arbeit mit Kaspersky Security Center in Amazon Web Services vorbereiten.

> Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Über die Arbeit in der Cloud-Umgebung Amazon Web Services

Sie können Kaspersky Security Center im AWS Marketplace in Form eines AMI-Image (Amazon Machine Image) erwerben, das ist ein einsatzbereites Abbild einer der vorläufig konfigurierten virtuellen Maschine. Sie können ein bezahltes AMI oder BYOL-AMI abonnieren und auf der Grundlage dieses Abbildes eine Amazon EC2-Instance mit installiertem Kaspersky Security Center Administrationsserver erstellen.

Für die Arbeit mit der AWS-Plattform und insbesondere, um die Apps in AWS Marketplace zu erwerben und Instanzen zu erstellen, benötigen Sie ein Benutzerkonto für Amazon Web Services. Sie können ein kostenloses Benutzerkonto auf https://aws.amazon.com/de erstellen. Sie können auch ein existierendes Benutzerkonto von Amazon verwenden.

Wenn Sie ein AMI abonniert haben, das in AWS Marketplace verfügbar ist, erhalten Sie eine Instance mit einsatzbereitem Kaspersky Security Center. Sie müssen das Programm nicht selbständig installieren. Der Kaspersky Security Center Administrationsserver wird in diesem Fall ohne Ihre Mitwirkung auf der Instanz installiert. Nach der Installation können Sie die Verwaltungskonsole starten und eine Verbindung mit dem Administrationsserver herstellen, um mit der Arbeit mit Kaspersky Security Center zu beginnen.

Informationen über das AMI und die Funktion des Online-Shops AWS Marketplace finden Sie auf der Hilfeseite von AWS Marketplace. Nähere Informationen zur Arbeit mit der Plattform AWS, zur Nutzung von Instances und zu den damit verbundenen Begriffen finden Sie in der Dokumentation zu Amazon Web Services.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Erstellen von IAM-Rollen und IAM-Benutzerkonten für Amazon EC2-Instances

In diesem Abschnitt werden die Aktionen beschrieben, die durchgeführt werden müssen, um einen ordnungsgemäßen Betrieb des Administrationsservers zu gewährleisten. Diese Aktionen umfassen Arbeiten mit den Rollen für AWS-Identität und Zugriffsverwaltung (IAM) und Benutzerkonten. Ferner werden die Aktionen beschrieben, die auf Client-Geräten unternommen werden müssen, um darauf den Administrationsagenten zu installieren und anschließen Kaspersky Security für Windows Server und Kaspersky Endpoint Security für Linux zu installieren.

Bereitstellung der Rechte für die Arbeit des Kaspersky Security Center Administrationsservers mit den AWS

Die Standards für den Betrieb in der Cloud-Umgebung Amazon Web Services schreiben vor, dass der Instance des Administrationsservers eine spezielle IAM-Rolle zum Arbeiten mit AWS-Diensten zugewiesen wird. Eine IAM-Rolle ist eine IAM-Entität, die den Satz der Berechtigungen für die Ausführung von Abfragen der AWS-Dienste definiert. Die IAM-Rolle verfügt über Berechtigungen zur Abfrage der Cloud-Segmente und zur Installation von Programmen auf Instances.

Nachdem Sie die IAM-Rolle erstellt und zum Administrationsserver ernannt haben, können Sie den Schutz von Instances bereitstellen, in dem Sie diese Rolle benutzen und Kaspersky Security Center keine Zusatzinformationen zur Verfügung stellen.

Es kann jedoch in folgenden Fällen zweckmäßig sein, auf das Erstellen der IAM-Rolle für den Administrationsserver zu verzichten:

- Die Geräte, deren Schutz Sie verwalten möchten, sind EC2-Instances innerhalb der Cloud-Umgebung der Amazon Web Services, aber der Administrationsserver befindet sich außerhalb der Umgebung.
- Wenn Sie planen, den Schutz von Instances nicht nur innerhalb Ihres Cloud-Segments, sondern auch innerhalb anderer Cloud-Segmente zu verwalten, die unter einem anderen Benutzerkonto in AWS erstellt wurden. In diesem Fall wird die IAM-Rolle nur für den Schutz Ihres Cloud-Segments benötigt. Für den Schutz der anderen Cloud-Segmente wird die IAM-Rolle nicht benötigt.

Für diese Fälle müssen Sie keine IAM-Rolle und kein *IAM-Benutzerkonto* erstellen, in dessen Namen Kaspersky Security Center mit den AWS-Diensten arbeiten soll. Bevor Sie die Arbeit mit dem Administrationsserver beginnen, erstellen Sie ein IAM-Benutzerkonto mit einem *AWS IAM-Zugriffsschlüssel* (im Weiteren auch als *IAM-Zugriffsschlüssel* bezeichnet).

Für das Erstellen der IAM-Rolle oder des IAM-Benutzerkontos ist die AWS-Managementkonsole erforderlich. Für die Arbeit mit der AWS-Managementkonsole werden der Benutzername und das Kennwort des Benutzerkontos in AWS benötigt.

IAM-Rolle für Administrationsserver erstellen

Erstellen Sie vor der Verteilung des Administrationsservers in der AWS-Managementkonsole die IAM-Rolle mit den erforderlichen Rechten für die Installation der Programme auf den Instances. Weitere Informationen finden Sie in der AWS-Hilfe in den Abschnitten über die IAM-Rollen.

Um eine IAM-Rolle für den Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die AWS-Managementkonsole und melden Sie sich mit dem AWS-Benutzerkonto an.
2. Erstellen Sie im Abschnitt **Rollen** eine Rolle mit den folgenden Berechtigungen:
   - **AmazonEC2ReadOnlyAccess**, wenn Sie nur die Abfrage von Cloud-Segmenten durchführen, aber keine Programme auf EC2-Instanzen mithilfe der AWS API installieren möchten.
   - **AmazonEC2ReadOnlyAccess** und **AmazonSSMFullAccess**, wenn Sie sowohl die Abfrage von Cloud-Segmenten als auch eine Installation von Programmen auf EC2-Instanzen mithilfe der AWS API vornehmen möchten. In diesem Fall benötigen Sie auf den geschützten EC2-Instanzen zusätzlich noch die IAM-Rolle mit den Rechten AmazonEC2RoleforSSM.

Sie müssen diese Rolle einer EC2-Instanz zuweisen, die Sie als Administrationsserver verwenden werden.

Die erstellte Rolle ist für alle Programme auf dem Administrationsserver verfügbar. Deshalb hat ein beliebiges Programm, das auf dem Administrationsserver läuft, die Möglichkeit, die Cloud-Segmente abzufragen oder Programme auf EC2-Instanzen innerhalb des Cloud-Segments zu installieren.

> Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Erstellen eines IAM-Benutzerkontos für die Arbeit mit Kaspersky Security Center

Zur Verwendung von Kaspersky Security Center ist ein IAM-Benutzerkonto erforderlich, wenn dem Administrationsserver keine IAM-Rolle mit den Rechten zur Gerätesuche und Installation von Programmen auf Instances zugewiesen wurde. Dasselbe Benutzerkonto oder ein anderes Benutzerkonto ist auch für die Aufgabe zum Backup der Daten des Administrationsservers erforderlich, wenn Sie einen S3-Bucket verwenden. Sie können ein IAM-Benutzerkonto mit allen erforderlichen Berechtigungen erstellen, oder Sie können zwei separate Benutzerkonten erstellen.

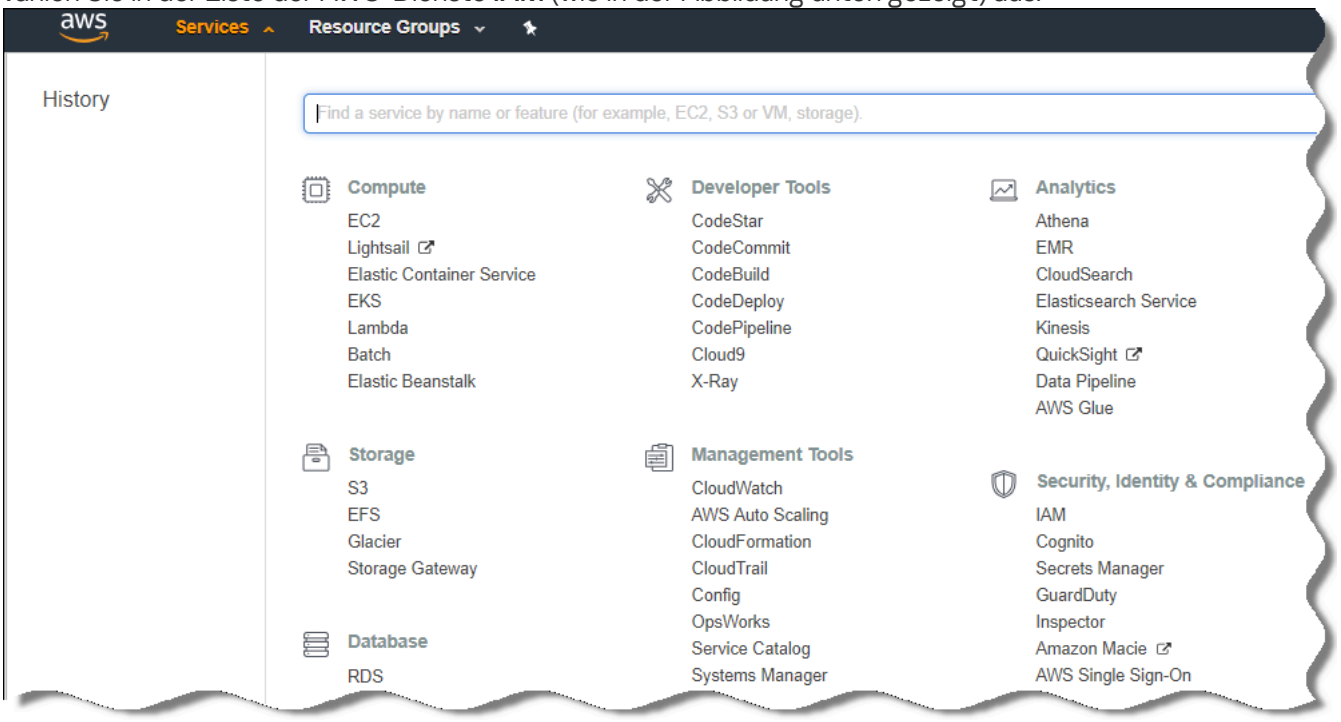
Für den IAM-Benutzer wird automatisch ein *IAM-Zugriffsschlüssel* erstellt, den Sie während der Erstkonfiguration für Kaspersky Security Center bereitstellen müssen. Der IAM-Zugriffsschlüssel besteht aus der ID des IAM-Zugriffsschlüssels und dem geheimen Schlüssel. Weitere Details zum IAM-Dienst finden Sie auf den folgenden Informationsseiten von AWS:

- http://docs.aws.amazon.com/de_de/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/de_de/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Um ein IAM-Benutzerkonto mit den erforderlichen Rechten zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die AWS-Managementkonsole und melden Sie sich mit dem Benutzerkonto an.

2. Wählen Sie in der Liste der AWS-Dienste **IAM** (wie in der Abbildung unten gezeigt) aus.



Liste der Dienste in der AWS-Managementkonsole

Es öffnet sich ein Fenster mit einer Liste von Benutzernamen und einem Menü für die Arbeit mit dem Tool.

3. Navigieren Sie durch die Bereiche der Konsole, die sich auf Benutzerkonten beziehen, und fügen Sie einen oder mehrere neue Benutzernamen hinzu.

4. Geben Sie für den/die hinzuzufügenden Benutzer die folgenden AWS-Eigenschaften an:

   - Zugriffstyp: **Befehlsorientierter Zugriff**.
   - Die Berechtigungsgrenze wurde nicht festgelegt.
   - Berechtigungen:
     - **ReadOnlyAccess**, wenn Sie nur die Abfrage von Cloud-Segmenten durchführen, aber keine Programme auf EC2-Instances mithilfe von AWS API installieren möchten.
     - **ReadOnlyAccess** und **AmazonSSMFullAccess**, wenn Sie sowohl die Abfrage von Cloud-Segmenten als auch eine Installation von Programmen auf EC2-Instances mithilfe von AWS API vornehmen möchten. In diesem Fall müssen Sie den geschützten EC2-Instances eine IAM-Rolle mit der Berechtigung AmazonEC2RoleforSSM zuweisen.

   Nachdem Sie Berechtigungen hinzugefügt haben, überprüfen Sie diese auf Genauigkeit. Gehen Sie im Fall einer irrtümlichen Auswahl zurück zum vorherigen Schirm und wiederholen Sie die Auswahl.

5. Nachdem Sie das Benutzerkonto erstellt haben, wird eine Tabelle mit dem IAM-Zugriffsschlüssel des neuen IAM-Benutzers angezeigt. Die ID des Zugriffsschlüssels wird in der Spalte **ID des Zugriffsschlüssels** angezeigt. Der geheime Schlüssel wird in der Spalte **Geheimer Zugriffsschlüssel** in Form von Sternchen angezeigt. Um den geheimen Schlüssel anzuzeigen, klicken Sie auf **Anzeigen**.

Das neu erstellte Benutzerkonto wird in der Liste der IAM-Benutzerkonten, die Ihrem Benutzerkonto in AWS entsprechen, angezeigt.

Bei der Bereitstellung von Kaspersky Security Center im Cloud-Segment müssen Sie festlegen, dass Sie das IAM-Benutzerkonto benutzen, und Kaspersky Security Center die ID des Zugriffsschlüssels und den geheimen Schlüssel bereitstellen.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Erstellen der IAM-Rolle für die Installation von Programmen auf Amazon EC2-Instances

Erstellen Sie vor der Bereitstellung des Schutzes auf EC2-Instances mithilfe von Kaspersky Security Center in der AWS-Managementkonsole die IAM-Rolle mit den erforderlichen Rechten für die Installation der Programme auf Instances. Weitere Informationen finden Sie in der AWS-Hilfe in den AWS-Hilfeabschnitten über die IAM-Rollen.

Die IAM-Rolle muss allen EC2-Instances zugewiesen werden, auf denen Sie Sicherheitsanwendungen mithilfe von Kaspersky Security Center installieren möchten. Wenn Sie einer Instance keine IAM-Rolle zuweisen, die über die erforderlichen Rechte verfügt, wird die Installation von Programmen mithilfe der AWS API auf dieser Instance mit einem Fehler beendet.

Für die Arbeit mit der AWS-Managementkonsole werden der Benutzername und das Kennwort des Benutzerkontos in AWS benötigt.

Um eine IAM-Rolle zur Installation des Programms auf Instances zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die AWS-Managementkonsole und melden Sie sich mit dem AWS-Benutzerkonto an.
2. Wählen Sie im Menü links den Punkt **Roles** aus.
3. Klicken Sie auf die Schaltfläche **Create Role**.
4. Wählen Sie in der angezeigten Liste mit Diensten **EC2** und anschließend in der Liste **Select Your Use** erneut **EC2** aus.
5. Klicken Sie auf **Next: Permissions**.
6. Aktivieren Sie in der angezeigten Liste das Kontrollkästchen neben **AmazonEC2RoleforSSM**.
7. Klicken Sie auf **Next: Review**.
8. Geben Sie den Namen und die Beschreibung der IAM-Rolle ein und klicken Sie auf die Schaltfläche **Create role**.

   Die erstellte Rolle wird in der Liste der Rollen mit dem von Ihnen angegebenen Namen und der Beschreibung angezeigt.

Im Weiteren können Sie die erstellte IAM-Rolle bei der Erstellung neuer EC2-Instances verwenden, die Sie mithilfe von Kaspersky Security Center schützen möchten, oder sie bereits vorhandenen Instances zuweisen.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Arbeiten mit Amazon RDS

In diesem Abschnitt wird beschrieben, welche Aktionen durchgeführt werden müssen, um eine Datenbank mithilfe von Amazon Relational Database Service (RDS) für Kaspersky Security Center vorzubereiten, sie in einer Optionsgruppe zu platzieren, eine IAM-Rolle zum Arbeiten mit RDS-Datenbank vorzubereiten, einen S3-Bucket zum Speichern vorzubereiten und eine bestehende Datenbank auf RDS zu migrieren.

Amazon RDS ist ein Webdienst, der AWS-Benutzern hilft, eine relationale Datenbank in der AWS-Cloud-Umgebung einzurichten, zu betreiben und zu skalieren. Wenn Sie möchten, können Sie eine Amazon RDS-Datenbank zum Arbeiten mit Kaspersky Security Center verwenden.

Sie können mit folgenden Datenbanken arbeiten:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Amazon RDS-Instance erstellen

Wenn Sie Amazon RDS als DBMS verwenden möchten, müssen Sie eine Amazon RDS-DB-Instance erstellen. Dieser Abschnitt beschreibt, wie Sie die SQL Express Edition auswählen. Wenn Sie mit Aurora MySQL oder Standard-MySQL (Versionen 5.7, 8.0) arbeiten möchten, müssen Sie eine dieser Engines auswählen.

Um eine Amazon RDS-DB-Instance zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die AWS-Managementkonsole auf https://console.aws.amazon.com und melden Sie sich mit Ihrem Benutzerkonto an.
2. Erstellen Sie mithilfe der AWS-Schnittstelle eine Datenbank mit den folgenden Einstellungen:
   - Modul: Microsoft SQL Server, SQL Express Edition
   - Version des DB-Moduls: SQL Server 2014 12.00.5546.0v1
   - Klasse der DB-Instanz: db.t2.medium
   - Speichertyp: Allgemeiner Zweck
   - Zugewiesener Speicher: mindestens 50 GB
   - Sicherheitsgruppe: die gleiche Gruppe, in der sich die EC2-Instance mit dem Kaspersky Security Center Administrationsserver befinden wird

   Erstellen Sie einen Identifikator, einen Benutzernamen und ein Kennwort für Ihre RDS-Instance.

Sie können die Standardeinstellungen in allen anderen Feldern unverändert lassen. Alternativ können Sie die Standardeinstellungen ändern, wenn Sie Ihre Amazon RDS-Instance anpassen möchten. Hilfe erhalten Sie auf den AWS-Informationsseiten.

3. Im letzten Schritt zeigt AWS die Ergebnisse des Prozesses an. Wenn Sie die Details Ihrer Amazon RDS-Instance anzeigen möchten, klicken Sie auf **Details der DB-Instance anzeigen**. Wenn Sie mit der nächsten Aktion fortfahren möchten, starten Sie mit dem Erstellen der Optionsgruppe für Ihre Amazon RDS-Instance.

Das Erstellen einer neuen Amazon RDS-Instance kann einige Minuten in Anspruch nehmen. Nachdem die Instance erstellt wurde, können Sie diese zum Arbeiten mit Daten von Kaspersky Security Center verwenden.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Optionsgruppe für eine Amazon RDS-Instance erstellen

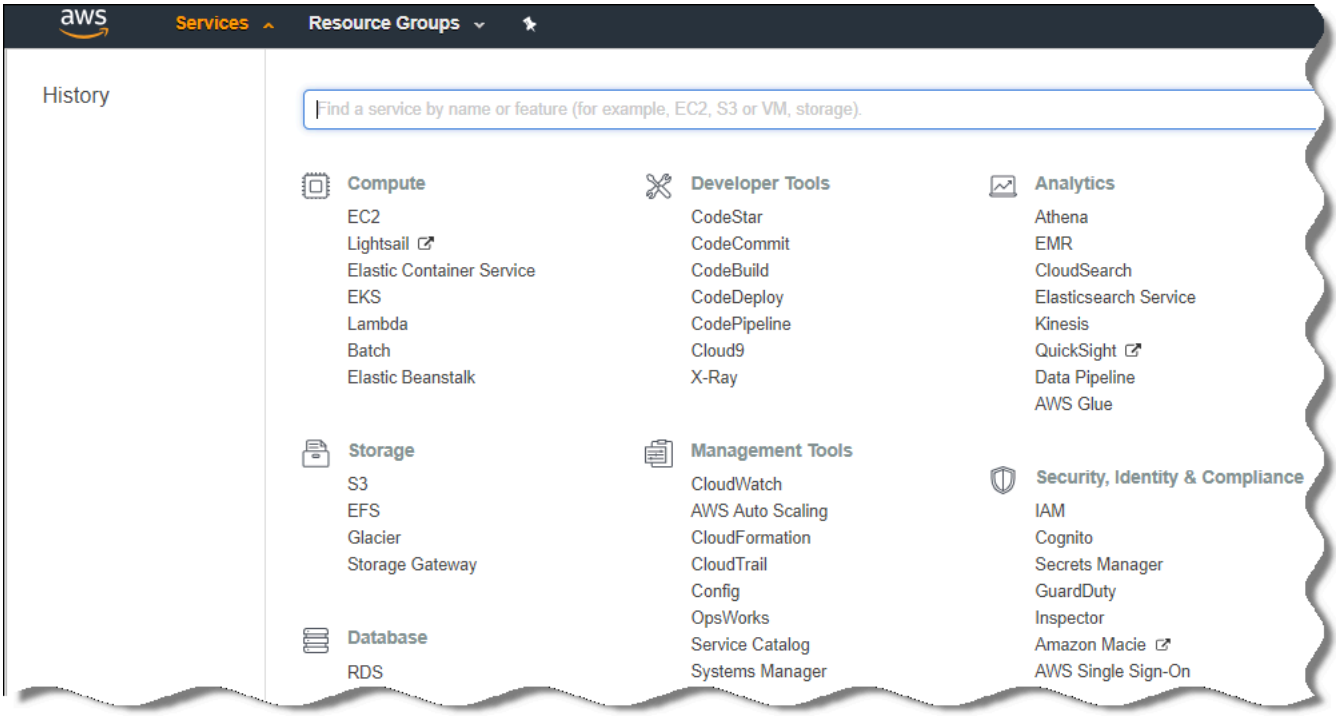
Sie müssen Ihre Amazon RDS-Instance in einer Optionsgruppe platzieren.

Um eine Optionsgruppe für Ihre Amazon RDS-Instance zu erstellen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie sich in der AWS-Managementkonsole befinden (https://console.aws.amazon.com) und mit Ihrem Benutzerkonto angemeldet sind.

2. Klicken Sie in der Menüzeile auf **Dienste**.

   Die Liste der verfügbaren Dienste wird angezeigt (siehe Abbildung unten).



Liste der Dienste in der AWS-Managementkonsole

3. Klicken Sie in der Liste auf **RDS**.

4. Klicken Sie im linken Bereich auf **Optionsgruppe**.

5. Klicken Sie auf die Schaltfläche **Gruppe erstellen**.

6. Erstellen Sie eine Optionsgruppe mit den folgenden Einstellungen, wenn Sie in der Phase zum Erstellen der Amazon RDS-Instance SQL Server ausgewählt haben:

   - Modul: SQLserver-ex
   - Modul-Hauptversion: 12.00

   Wenn Sie in der Phase zum Erstellen der Amazon RDS-Instance eine andere SQL-Datenbank ausgewählt haben, wählen Sie ein entsprechendes Modul.

   Daraufhin wird die Gruppe in der Liste mit Ihren Gruppen erstellt und angezeigt.

Nach dem Erstellen der Optionsgruppe platzieren Sie Ihre Amazon RDS-Instance in diese Optionsgruppe.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Ändern der Optionsgruppe

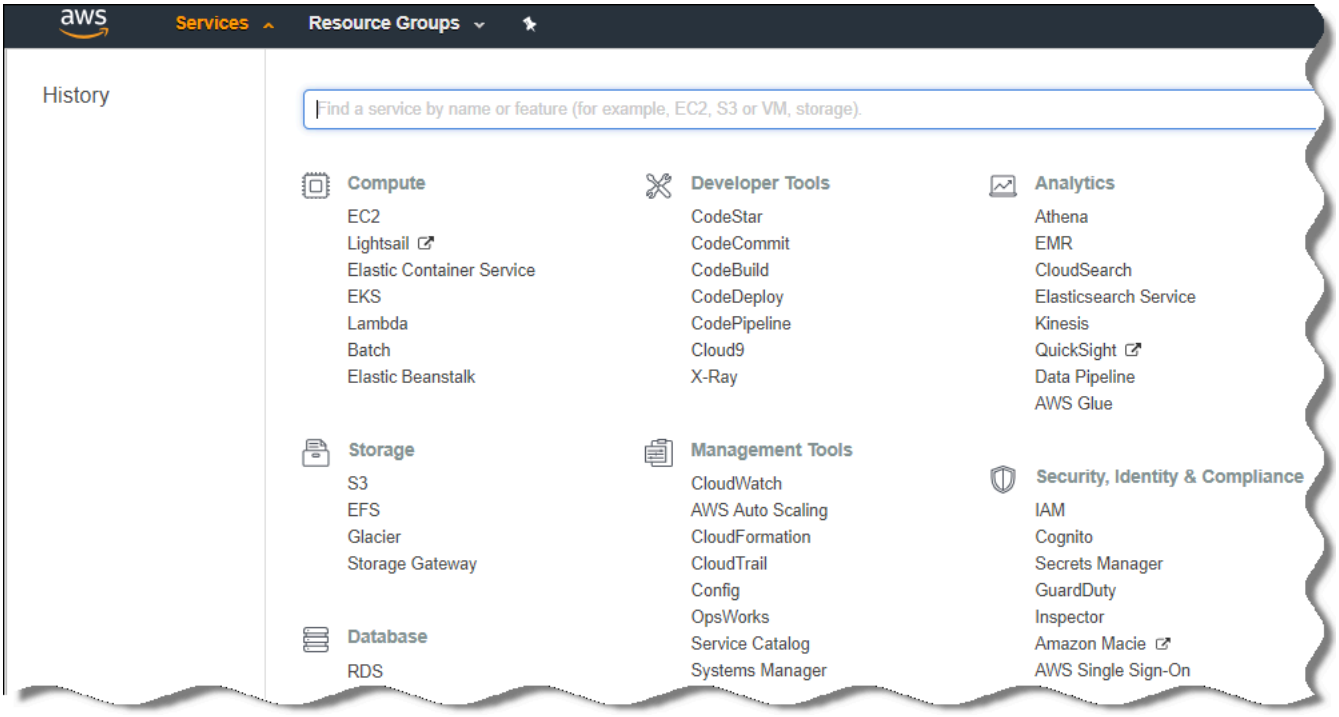
Die Standardkonfiguration der Optionsgruppe, in der Sie die Amazon RDS-Instanz platziert haben, reicht nicht aus, um sie mit der Kaspersky Security Center-Datenbank zu verwenden. Sie müssen Optionen zur Optionsgruppe hinzufügen und eine neue IAM-Rolle zur Verwendung der Datenbank erstellen.

Um die Optionsgruppe zu ändern und eine neue IAM-Rolle zu erstellen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie sich in der AWS-Managementkonsole befinden (https://console.aws.amazon.com) und mit Ihrem Benutzerkonto angemeldet sind.

2. Klicken Sie in der Menüzeile auf **Dienste**.

   Die Liste der verfügbaren Dienste wird angezeigt (siehe Abbildung unten).



Liste der Dienste in der AWS-Managementkonsole

3. Wählen Sie in der Liste RDS aus.

4. Klicken Sie im linken Bereich auf **Optionsgruppe**.

   Die Liste der Optionsgruppe wird angezeigt.

5. Wählen Sie die Optionsgruppe aus, in der Sie die Amazon RDS-Instanz platziert haben und klicken Sie auf die Schaltfläche **Option hinzufügen**.

   Das Fenster **Option hinzufügen** wird geöffnet.

6. Wählen Sie im Abschnitt "IAM-Rolle" die Option **Neue Rolle erstellen** / **Ja** und geben Sie einen Namen für die neue IAM-Rolle ein.

   Die Rolle wird mit einem Standardsatz von Berechtigungen erstellt. Später müssen Sie deren Berechtigungen ändern.

7. Führen Sie im Abschnitt "S3-Bucket" eine der folgenden Aktionen aus:

   - Wenn Sie keine Amazon S3-Bucket-Instanz als Daten-Backup erstellt haben, wählen Sie den Link **Neuen S3-Bucket erstellen** und erstellen Sie mithilfe der AWS-Benutzeroberfläche einen neuen S3-Bucket aus.

   - Wenn Sie bereits eine Amazon S3-Bucket-Instanz für die Aufgabe zum Erstellen eines Daten-Backups des Administrationsservers erstellt haben, wählen Sie Ihren S3-Bucket aus der Dropdown-Liste aus.

8. Schließen Sie die Optionen für das Hinzufügen ab, indem Sie auf die Schaltfläche **Option hinzufügen** im unteren Bereich der Seite klicken.

Sie haben die Optionsgruppe geändert und eine neue IAM-Rolle zum Arbeiten mit der RDS-Datenbank erstellt.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Ändern der Berechtigungen für die IAM-Rolle der Amazon RDS-DB-Instance

Nach dem Hinzufügen von Optionen zu der Optionsgruppe, müssen Sie die erforderlichen Berechtigungen der IAM-Rolle zuweisen, die Sie zum Arbeiten mit der Amazon RDS-DB-Instance erstellt haben.

Um die erforderlichen Berechtigungen der IAM-Rolle, die Sie zum Arbeiten mit der Amazon RDS-DB-Instance erstellt haben, zuzuweisen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie sich in der AWS-Managementkonsole befinden (https://console.aws.amazon.com) und mit Ihrem Benutzerkonto angemeldet sind.

2. Wählen Sie in der Liste der Dienste **IAM** aus.

   Es öffnet sich ein Fenster mit einer Liste von Benutzernamen und einem Menü für die Arbeit mit dem Tool.

3. Wählen Sie im Menü **Rollen** aus.

4. Wählen Sie in der Liste der IAM-Rollen im Arbeitsbereich die Rolle aus, die Sie erstellt haben, als Sie die Option zu Optionsgruppe hinzugefügt haben.

5. Löschen Sie mithilfe der AWS-Benutzeroberfläche die Richtlinie **sqlNativeBackup-<Datum>**.

6. Fügen Sie mithilfe der AWS-Benutzeroberfläche die Richtlinie **AmazonS3FullAccess** zur Rolle hinzu.

   Die IAM-Rolle erhält die erforderlichen Berechtigungen zum Arbeiten mit Amazon RDS.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Amazon S3-Bucket für Datenbank vorbereiten

Wenn Sie vorhaben, eine Amazon Relational Database Service (Amazon RDS)-Datenbank zu verwenden, müssen Sie eine Amazon Simple Storage Service (Amazon S3)-Bucket-Instance erstellen, in der das regelmäßige Backup der Datenbank gespeichert wird. Informationen über Amazon S3 und S3-Buckets finden Sie auf den Amazon-Hilfeseiten. Weitere Informationen zum Erstellen einer Amazon S3-Instance finden Sie Hilfeseite zu Amazon S3.

Um einen Amazon S3-Bucket zu erstellen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die AWS-Managementkonsole geöffnet ist und Sie mit Ihrem Benutzerkonto angemeldet sind.

2. Wählen Sie in der Liste der AWS-Dienste S3 aus.

3. Navigieren Sie in der Konsole, um einen Bucket zu erstellen und folgen Sie dabei den Anweisungen des Assistenten.

4. Wählen Sie dieselbe Region aus, in der sich Ihr Administrationsserver befindet (oder sich befinden wird).

5. Stellen Sie nach der Beendung des Assistenten sicher, dass der neue Bucket in der Liste der Buckets angezeigt wird.

   Daraufhin wird ein neuer S3-Bucket erstellt und in Ihrer Liste der Buckets angezeigt. Sie müssen diesen Bucket festlegen, wenn Sie Optionen zur Optionsgruppe hinzufügen. Sie müssen ferner die Adresse Ihres S3-Buckets für Kaspersky Security Center festlegen, wenn Kaspersky Security Center die Aufgabe *Backup der Daten des Administrationsservers* erstellt.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Datenbank auf Amazon RDS migrieren

Sie können Ihre Datenbank für Kaspersky Security Center von einem Gerät vor Ort auf eine Amazon S3-Instance migrieren, die Amazon RDS unterstützt. Dazu benötigen Sie einen S3-Bucket für eine RDS-Datenbank und ein IAM-Benutzerkonto mit AmazonS3FullAccess-Berechtigung für diesen S3-Bucket.

Um die Migration der Datenbank durchzuführen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie eine RDS-Instance erstellt haben (Details finden Sie auf den Amazon RDS-Referenzseiten).

2. Führen Sie auf Ihrem physikalischen Administrationsserver (vor Ort) das Kaspersky-Backup-Tool aus, um die Daten des Administrationsservers zu sichern.

   Stellen Sie sicher, dass die Datei backup.zip heißt.

3. Kopieren Sie die Datei backup.zip in die EC2-Instanz, auf welcher der Administrationsserver installiert ist.

   > Stellen Sie sicher, dass Sie über genügend Speicherplatz auf der EC2-Instance verfügen, auf welcher der Administrationsserver installiert ist. In der AWS-Umgebung können Sie Speicherplatz zu Ihrer Instance hinzufügen, um sie für den Prozess der Datenbankmigration zu anzupassen.

4. Starten Sie auf dem AWS-Administrationsserver das Kaspersky-Backup-Tool erneut im interaktiven Modus.

   Der Backup- und Wiederherstellungsassistent wird gestartet.

5. Wählen Sie im Schritt **Wählen Sie eine Aktion aus** den Punkt **Wiederherstellen der Daten des Administrationsservers** und klicken Sie auf **Weiter**.

6. Klicken Sie im Schritt **Einstellungen für Wiederherstellung** auf die Schaltfläche **Durchsuchen** neben dem **Ordner für Backup-Kopien**.

7. Füllen Sie in dem sich öffnenden Fenster **Bei Cloud-Speicher anmelden** die folgenden Felder aus und klicken Sie auf **OK**:

   - **Name des S3-Buckets**

     Der Name Ihres S3-Buckets.

   - **Backup-Ordner**

     Legen Sie den Speicherort des Ordners fest, der für das Backup vorgesehen ist.

   - **ID des Zugriffsschlüssels**

     Geben Sie die ID des AWS IAM-Zugriffsschlüssels ein, der zum IAM-Benutzer gehört, der über die Berechtigungen zur Verwendung des S3-Buckets verfügt (die Berechtigung AmazonS3FullAccess).

   - **Geheimer Schlüssel**

     Geheimer AWS IAM-Zugriffsschlüssel, der zum IAM-Benutzer gehört, der über die Berechtigungen zur Verwendung des S3-Buckets verfügt (die Berechtigung AmazonS3FullAccess).

8. Wählen Sie die Option **Von lokalem Backup migrieren** aus. Die Schaltfläche **Auswählen** wird verfügbar.

9. Klicken Sie auf **Durchsuchen**, um den Ordner auf dem AWS-Administrationsserver auszuwählen, in den Sie die Datei backup.zip kopiert haben.

10. Klicken Sie auf **Weiter** und schließen Sie den Vorgang ab.

    Ihre Daten werden mithilfe Ihres S3-Buckets in der RDS-Datenbank wiederhergestellt. Sie können diese Datenbank zum weiteren Arbeiten mit Kaspersky Security Center in der AWS-Umgebung verwenden.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Arbeiten mit der Cloud-Umgebung Microsoft Azure

Dieser Abschnitt informiert über die Bereitstellung und Wartung von Kaspersky Security Center in einer Cloud-Umgebung, die von Microsoft Azure bereitgestellt wird, sowie über die Bereitstellung des Schutzes auf virtuellen Maschinen in dieser Cloud-Umgebung.

Wenn Kaspersky Security Center mit einem nutzungsbasierten, monatlich verrechneten SKU verteilt wurde, wird "Schwachstellen- und Patch-Management" automatisch aktiviert, während die Komponente "Mobile Geräte verwalten" nicht aktiviert werden kann.

Über das Arbeiten in Microsoft Azure

Für das Arbeiten mit der Plattform Microsoft Azure und insbesondere, um Apps im Azure Marketplace zu kaufen und virtuelle Maschinen zu erstellen, benötigen Sie ein Azure-Abonnement. Bevor Sie den Administrationsserver verteilen, erstellen Sie eine Anwendungs-ID für Azure mit Berechtigungen, die für die Installation von Apps auf virtuellen Maschinen erforderlich sind.

Wenn Sie ein Abbild von Kaspersky Security Center im Azure Marketplace kaufen, können Sie eine virtuelle Maschine mit Ihrem einsatzbereiten Kaspersky Security Center Administrationsserver verteilen. Sie müssen Einstellungen der virtuellen Maschine auswählen, aber Sie müssen die Anwendung nicht selbst installieren. Nach der Installation können Sie die Verwaltungskonsole starten und eine Verbindung mit dem Administrationsserver herstellen, um mit der Arbeit mit Kaspersky Security Center zu beginnen.

Sie können auch eine virtuelle Maschine von Azure mit dem darauf verteilten Kaspersky Security Center Administrationsserver verwenden, um Geräte vor Ort zu schützen (zum Beispiel, wenn sich herausstellt, dass ein Cloud-Server vorteilhafter in der Bedienung und in Bezug auf den Inhalt ist, als ein physischer). In diesem Fall wird die Arbeit mit dem Administrationsserver genauso konfiguriert wie wenn der Administrationsserver auf einem Gerät vor Ort installiert wäre. Wenn Sie nicht vorhaben, Azure API-Tools zu verwenden, benötigen Sie keine Anwendungs-ID für Azure. In diesem Fall reicht ein Azure-Abonnement aus.

Erstellen eines Abonnements, einer Anwendungs-ID und eines Kennworts

Zum Arbeiten mit Kaspersky Security Center in der Microsoft Azure-Umgebung benötigen Sie ein Azure-Abonnement, eine Anwendungs-ID für Azure und ein Azure Anwendungs-Kennwort. Sie können ein bestehendes Abonnement verwenden, wenn Sie bereits über eines verfügen.

Ein Azure-Abonnement gewährt seinem Inhaber Zugriff auf das Verwaltungsportal der Microsoft Azure-Plattform und auf die Microsoft Azure-Dienste. Der Inhaber kann die Microsoft Azure-Plattform verwenden, um Dienste wie Azure SQL, Azure Storage zu verwalten.

Um ein Microsoft Azure-Abonnement zu erstellen,

Wechseln Sie auf https://learn.microsoft.com/de-de/azure/cost-management-billing/manage/create-subscription und folgen Sie dort den Anweisungen.

Weitere Informationen über das Erstellen eines Abonnements finden Sie auf der Website von Microsoft. Sie erhalten eine Abonnement-ID, die Sie später gemeinsam mit der Anwendungs-ID und dem Kennwort für Kaspersky Security Center bereitstellen.

So erstellen und speichern Sie eine Azure Anwendungs-ID und ein Anwendungs-Kennwort:

1. Wechseln Sie zu https://portal.azure.com und stellen Sie sicher, dass Sie angemeldet sind.
2. Folgen Sie den Anweisungen auf der Referenzseite, um Ihre Anwendungs-ID zu erstellen.
3. Wechseln Sie zum Abschnitt **Schlüssel** in den Programmeinstellungen.
4. Füllen Sie im Abschnitt **Schlüssel** die Felder **Beschreibung** und **Läuft ab** aus und lassen Sie das Feld **Wert** leer.
5. Klicken Sie auf **Speichern**.

   Sobald Sie auf **Speichern** klicken, trägt das System im Feld **Wert** automatisch eine lange Zeichenfolge ein. Diese Zeichenfolge ist Ihr Azure-App-Kennwort (beispielsweise yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). Die Beschreibung wird wie von Ihnen eingegeben angezeigt.
6. Kopieren Sie das Kennwort und bewahren Sie es auf, um es Kaspersky Security Center später zusammen mit der Anwendungs-ID bereitzustellen.

   Sie können das Kennwort nur nach seiner Erstellung kopieren. Zu einem späteren Zeitpunkt wird das Kennwort nicht mehr angezeigt und kann nicht wiederhergestellt werden.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Der Azure Anwendungs-ID eine Rolle zuweisen

Wenn Sie lediglich virtuelle Maschinen mithilfe der Gerätesuche ermitteln möchten, muss Ihre Azure Anwendungs-ID über die Rolle "Reader" verfügen. Wenn Sie die virtuellen Maschinen nicht nur finden, sondern auch schützen möchten, muss Ihre Anwendungs-ID für Azure die Rolle "Mitwirkender für virtuelle Computer" haben.

Befolgen Sie die Anleitung auf der Microsoft-Website, um Ihrer Azure Anwendungs-ID eine Rolle zuzuweisen.

Verteilen des Administrationsservers in Microsoft Azure und Auswählen der Datenbank

Um den Administrationsserver in der Microsoft Azure-Umgebung zu verteilen, gehen Sie wie folgt vor:

1. Melden Sie sich mit Ihrem Benutzerkonto bei Microsoft Azure an.
2. Wechseln Sie zum Azure-Portal.
3. Klicken Sie im linken Bereich auf das grüne Plus-Symbol.
4. Tippen Sie "Kaspersky Hybrid Cloud Security" in das Suchfeld im Menü ein.

   Kaspersky Hybrid Cloud Security ist eine Kombination von Kaspersky Security Center und zweier Sicherheitsanwendungen zum Schutz von Instances: Kaspersky Endpoint Security für Linux und Kaspersky Security für Windows Server.
5. Wählen Sie in der Liste der Ergebnisse Kaspersky Hybrid Cloud Security oder Kaspersky Hybrid Cloud Security (BYOL) aus.

   Daraufhin wird im rechten Teil des Schirms ein Informationsfenster angezeigt.
6. Lesen Sie die Informationen und klicken Sie auf die Schaltfläche "Erstellen" am Ende des Informationsfensters.
7. Füllen Sie alle erforderlichen Felder aus. Nutzen Sie die Tooltipps, um Informationen und Hilfe zu erhalten.
8. Wählen Sie bei der Auswahl der Größe eine der drei Optionen mit Stern.

   In den meisten Fällen sind 8 Gigabyte (GB) Arbeitsspeicher ausreichend. In Azure können Sie jedoch die Größe des Arbeitsspeichers und anderer Ressourcen der virtuelle Maschinen Maschine jederzeit erhöhen.
9. Wählen Sie bei der Auswahl der Datenbank eine der folgenden gemäß Ihrem Plan aus:

   - Lokal – Wenn Sie eine Datenbank auf derselben virtuellen Maschine möchten, auf welcher der Administrationsserver bereitgestellt wird. Kaspersky Security Center wird mit einer SQL Server Express ausgeliefert. Wählen Sie diese Option, wenn SQL Server Express für Ihre Bedürfnisse ausreichend ist.
   - Neu – Wenn Sie eine neue RDS-Datenbank in der Azure-Umgebung möchten. Wählen Sie diese Option, wenn Sie ein anderes DBMS als SQL Server Express verwenden möchten. Ihre Daten werden an die Cloud-Umgebung übertragen, wo sie verbleiben, und Sie haben keine zusätzlichen Ausgaben.
   - Bestehend – Wenn Sie einen bestehenden Datenbankserver verwenden möchten. In diesem Fall müssen Sie dessen Ort festlegen. Wenn sich dieser Server außerhalb der Azure-Umgebung befindet, werden Ihre Daten über das Internet übertragen, was zu Zusatzkosten führen kann.
10. Verwenden Sie beim Eingeben der Abonnement-ID das zuvor erstellte Abonnement.

Nach der Bereitstellung können Sie eine Verbindung zum Administrationsserver über RDP herstellen. Sie können die Verwaltungskonsole zum Arbeiten mit dem Administrationsserver nutzen.

Mit Azure SQL arbeiten

In diesem Abschnitt wird beschrieben, welche Aktionen ausgeführt werden müssen, um eine Microsoft Azure-Datenbank für Kaspersky Security Center vorzubereiten, ein Azure-Speicherkonto vorzubereiten und eine vorhandene Datenbank nach Azure SQL zu migrieren.

SQL Database ist ein verwalteter Allzweck-Service für relationale Datenbanken in Microsoft Azure.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Azure-Speicherkonto erstellen

Sie benötigen ein Speicherkonto in Microsoft Azure, um die Azure SQL-Datenbank und Bereitstellungsskripte verwenden zu können.

So erstellen Sie ein Speicherkonto:

1. Melden Sie sich im Azure-Portal an.
2. Klicken Sie im linken Bereich auf **Speicherkonten**, um zum Fenster **Speicherkonten** zu wechseln.
3. Drücken Sie im Fenster **Speicherkonten** auf die Schaltfläche **Hinzufügen**, um zum Fenster **Speicherkonto erstellen** zu wechseln.
4. Füllen Sie alle erforderlichen Felder aus, um ein Speicherkonto zu erstellen:
   - Ort: Muss mit dem Standort des Administrationsservers übereinstimmen.
   - Andere Felder: Sie können die Standardwerte belassen.

   Nutzen Sie die Tooltipps, um Informationen zu allen Feldern abzurufen.

   Nachdem das Speicherkonto erstellt wurde, wird die Liste Ihrer Speicherkonten angezeigt.
5. Klicken Sie in der Liste Ihrer Speicherkonten auf den Namen des neu erstellten Kontos, um Informationen zu diesem Konto anzuzeigen.
6. Stellen Sie sicher, dass Sie den Benutzerkonto-Namen, die Ressourcengruppe und die Zugriffsschlüssel für dieses Speicherkonto kennen. Sie benötigen diese Informationen für die Arbeit mit Kaspersky Security Center.

Hilfe finden Sie auf der Azure-Website.

Wenn Sie bereits über ein Speicherkonto verfügen, können Sie es für die Arbeit mit Kaspersky Security Center verwenden.

Azure SQL-Datenbank und SQL Server erstellen

Sie benötigen eine SQL-Datenbank und SQL Server in der Azure-Umgebung.

So erstellen Sie eine Azure SQL-Datenbank und einen SQL-Server:

1. Folgen Sie den Anweisungen auf der Azure-Website.

   Sie können einen neuen Server erstellen, sobald Sie von Microsoft Azure dazu aufgefordert werden; sollten Sie bereits einen Azure SQL-Server haben, können Sie diesen für Kaspersky Security Center verwenden, ohne einen neuen erstellen zu müssen.

2. Stellen Sie nach dem Erstellen der SQL-Datenbank und SQL Server sicher, dass Sie den Ressourcennamen und die Ressourcengruppe kennen:

   a. Wechseln Sie zu https://portal.azure.com und stellen Sie sicher, dass Sie angemeldet sind.

   b. Wählen Sie im linken Fensterbereich die Option **SQL-Datenbanken** aus.

   c. Klicken Sie in der Liste Ihrer Datenbanken auf den Namen der Datenbank.

      Daraufhin wird das Eigenschaftenfenster geöffnet.

   d. Der Name der Datenbank ist der Ressourcenname. Der Name der Ressourcengruppe wird im Abschnitt **Übersicht** des Fensters Eigenschaften angezeigt.

Sie müssen den Namen der Ressource und Ressourcengruppe der Datenbank angeben, um die Datenbank zur Azure SQL zu migrieren.

Datenbank auf Azure SQL migrieren

Nach der Bereitstellung des Administrationsservers in der Azure-Umgebung können Sie Ihre Kaspersky Security Center-Datenbank von einem Gerät vor Ort auf Azure SQL migrieren. Sie benötigen ein Azure-Speicherkonto für eine Azure SQL-Datenbank. Auf Ihrem Administrationsserver müssen außerdem Microsoft SQL Server Data-Tier Application Framework (DacFx) und SQLSysCLRTypes vorhanden sein.

Um die Migration der Datenbank durchzuführen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie ein Azure-Speicherkonto erstellt haben.

2. Achten Sie darauf, dass Sie SQLSysCLRTypes und DacFx auf Ihrem Administrationsserver installiert haben.

   Sie können Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) und SQLSysCLRTypes (wählen Sie die Version aus, die der Version Ihres SQL Servers entspricht) von der offiziellen Microsoft-Website herunterladen.

3. Führen Sie auf Ihrem physikalischen Administrationsserver (vor Ort) das Kaspersky-Backup-Tool aus, um die Daten des Administrationsservers mit aktivierter Option **Auf Azure-Format migrieren** zu sichern.

4. Kopieren Sie die Backup-Datei auf den Azure-Administrationsserver.

   > Stellen Sie sicher, dass auf der virtuellen Azure-Maschine, auf welcher der Administrationsserver installiert ist, ausreichend Speicherplatz vorhanden ist. In der Azure-Umgebung können Sie Ihren virtuellen Maschinen Festplattenspeicher hinzufügen, um den Prozess der Datenbankmigration zu unterstützen.

5. Starten Sie auf dem Administrationsserver in der Microsoft Azure-Umgebung das Kaspersky-Backup-Tool erneut im interaktiven Modus.

   Der Backup- und Wiederherstellungsassistent wird gestartet.

6. Wählen Sie im Schritt **Wählen Sie eine Aktion aus** den Punkt **Wiederherstellen der Daten des Administrationsservers** und klicken Sie auf **Weiter**.

7. Klicken Sie im Schritt **Einstellungen für Wiederherstellung** auf die Schaltfläche **Durchsuchen** neben dem **Ordner für Backup-Kopien**.

8. Füllen Sie in dem sich öffnenden Fenster **Bei Cloud-Speicher anmelden** die folgenden Felder aus und klicken Sie auf **OK**:

   - **Name des Azure-Speicherkontos**

     Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

   - **Backup-Ordner**

     Legen Sie den Speicherort des Ordners fest, der für das Backup vorgesehen ist.

   - **Azure-Abonnement-ID**

     Sie haben das Abonnement auf dem Azure-Portal erstellt.

   - **Azure-App-Kennwort**

     Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

     Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

   - **Zugriffsschlüssel für Azure-Speicher**

     Verfügbar in den Eigenschaften Ihres Speicherkontos im Abschnitt "Zugriffsschlüssel". Sie können einen der Schlüssel (Schlüssel1 oder Schlüssel2) verwenden.

   - **Name des Azure SQL-Servers**

     Verfügbar in den Eigenschaften Ihres Azure SQL-Servers.

   - **Azure SQL-Serverressourcengruppe**

     Verfügbar in den Eigenschaften Ihres Azure SQL-Servers.

   - **Anwendungs-ID für Azure**

     Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

     Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

9. Wählen Sie die Option **Von lokalem Backup migrieren** aus.

   Die Schaltfläche **Auswählen** wird verfügbar.

10. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den Ordner auf dem Azure-Administrationsserver zu schließen, in den Sie die Backup-Datei kopiert haben.

11. Klicken Sie auf **Weiter** und schließen Sie den Vorgang ab.

Ihre Daten werden mithilfe Ihres Azure-Speichers in der Azure SQL-Datenbank wiederhergestellt. Sie können diese Datenbank zum weiteren Arbeiten mit Kaspersky Security Center in der Azure-Umgebung verwenden.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center aktuell.

Arbeiten mit Google Cloud

Dieser Abschnitt enthält Informationen über das Arbeiten mit Kaspersky Security Center in einer von Google bereitgestellten Cloud-Umgebung.

Erstellen von Client-E-Mail, Projekt-ID und privatem Schlüssel

Sie können die Google API verwenden, um mit Kaspersky Security Center in der Google Cloud-Plattform zu arbeiten. Dafür wird ein Google-Benutzerkonto benötigt. Weitere Informationen entnehmen Sie bitte der Dokumentation von Google unter https://cloud.google.com.

Die folgenden Informationen müssen Sie erstellen und in Kaspersky Security Center zur Verfügung stellen:

- **Client-E-Mail**

  Client-E-Mail ist die E-Mail-Adresse, die Sie für Ihr Projekt bei Google Cloud registriert haben.

- **Projekt-ID**

  Projekt-ID ist die ID, die Sie erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben.

- **Privater Schlüssel**

  Privater Schlüssel ist die Zeichenfolge, die Sie als privaten Schlüssel erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben. Um Fehler zu vermeiden können Sie die Zeichenfolge kopieren und einfügen.

Arbeiten mit einer Instanz von Google Cloud SQL for MySQL

Sie können in Google Cloud eine Datenbank anlegen und für Kaspersky Security Center verwenden.

Kaspersky Security Center unterstützt MySQL 5.7 und 5.6. Andere Versionen von MySQL wurden nicht getestet.

Um eine MySQL-Datenbank anzulegen und zu konfigurieren:

Öffnen Sie in Ihrem Browser die Seite https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen und folgen Sie den Anweisungen.

Verwenden Sie bei der Konfiguration einer MySQL-Datenbank die folgenden Flags:

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000

- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

Erforderliche Komponenten für Client-Geräte in einer Cloud-Umgebung für die Arbeit mit Kaspersky Security Center

Die Geräte, auf denen Sie planen, den Administrationsserver, den Administrationsagenten und die Sicherheitsanwendungen von Kaspersky zu installieren, müssen die folgenden Bedingungen erfüllen:

- Die Einstellungen der Sicherheitsgruppen machen folgende Ports auf dem Administrationsserver verfügbar (für die Bereitstellung mindestens benötigte Reihe an Ports):
  - 8060 HTTP (zur Übermittlung von Installationspaketen des Administrationsagenten und der Sicherheitsanwendungen vom Administrationsserver an die geschützten Instances)
  - 8061 HTTPS (zur Übermittlung von Installationspaketen des Administrationsagenten und der Sicherheitsanwendungen vom Administrationsserver an die geschützten Instances)
  - 13000 TCP (zur Übermittlung von den geschützten Instanzen und den sekundären Administrationsservern an den primären Administrationsserver mittels SSL)
  - 13000 UDP (zur Übermittlung von Informationen über die Deaktivierung von Instances an den Administrationsserver)
  - 14000 TCP (zur Übermittlung von den geschützten Instanzen und den sekundären Administrationsservern an den primären Administrationsserver ohne SSL)
  - 13291 (für die Verbindung der Verwaltungskonsole mit dem Administrationsserver verwendet)
  - 40080 (für den Betrieb von Scripts zur Bereitstellung)

  Sie können die Sicherheitsgruppen in der AWS-Managementkonsole oder auf dem Azure-Portal anpassen. Wenn Sie Kaspersky Security Center nicht in der Standard-Konfiguration verwenden möchten, finden Sie weitere Informationen dazu in der Wissensdatenbank. Beispiele für eine nicht standardmäßige Konfiguration sind: Installation der Verwaltungskonsole nicht auf dem Gerät mit dem Administrationsserver, sondern am eigenen Arbeitsplatz, oder die Verwendung eines KSN-Proxyservers.
- Auf den Client-Geräten ist der Port 15000 UDP verfügbar (zur Annahme von Verbindungsanfragen vom Administrationsserver).

- In der Cloud-Umgebung von AWS:
  - Wenn Sie vorhaben, die AWS API zu verwenden, wird die IAM-Rolle eingerichtet, unter der die Programme auf den Instances installiert werden.
  - Auf jeder Amazon EC2-Instance wird der Systems Manager Agent (SSM-Agent) installiert und ausgeführt.
  - Der SSM-Agent erlaubt Kaspersky Security Center, Programme automatisch auf den Geräten und Gerätegruppen zu installieren, ohne jedes Mal eine Bestätigung durch einen Administrator abzufragen.
  - Auf Instanzen unter Verwaltung des Betriebssystems Windows, die mithilfe von AMI-Images nach November 2016 verteilt wurden, ist der SSM-Agent installiert und funktioniert. Auf allen übrigen Geräten müssen Sie den SSM-Agenten selbständig installieren. Weitere Informationen zur Installation des SSM-Agenten auf Geräte unter Verwaltung der Betriebssysteme Windows und Linux finden Sie auf der AWS-Hilfeseite.
- In der Microsoft Azure Cloud-Umgebung:
  - Auf jeder Azure virtuellen Maschine wird der Azure VM Agent installiert und ausgeführt.

    Standardmäßig wird eine neue virtuelle Maschine mit Azure VM Agent erstellt und Sie müssen sie nicht installieren oder manuell aktivieren. Details zum Azure VM Agent auf Windows-Geräten und auf Linux-Geräten finden Sie in den Hilfeseiten von Microsoft.
  - Ihre Anwendungs-ID für Azure besitzt die folgenden Rollen:
    - Leser (zum Erkennen virtueller Maschinen mittels Abfrage)
    - Mitwirkender für virtuelle Computer (zum Verteilen des Schutzes auf virtuellen Maschinen)
    - SQL Server-Mitwirkender (zur Verwendung einer SQL-Datenbank in der Microsoft Azure-Umgebung)

    Wenn Sie in der Lage sein möchten, alle drei Aktionen auszuführen, weisen Sie Ihrer Anwendungs-ID für Azure alle drei Rollen zu.

Erstellen von Installationspaketen, die zur Konfiguration der Cloud-Umgebung erforderlich sind

Der Assistent zur Konfiguration der Cloud-Umgebung ist in Kaspersky Security Center verfügbar, wenn Sie über die Installationspakete und Verwaltungs-Plug-ins der folgenden Programme verfügen:

- Kaspersky Endpoint Security für Linux
- Kaspersky Endpoint Security für Windows

  Das Bereitstellen von Kaspersky Endpoint Security für Windows in einer Cloud-Umgebung wird nach der bevorstehenden Veröffentlichung von Kaspersky Endpoint Security 12.0 für Windows verfügbar sein.
- Kaspersky Security für Windows Server

Die folgenden Installationspakete sind erforderlich für die Installation der Anwendungen auf den Instanzen oder virtuellen Maschinen, die Sie schützen möchten. Wenn Sie nicht über die Installationspakete verfügen, müssen Sie diese erstellen. Andernfalls funktioniert Assistent zur Konfiguration der Cloud-Umgebung nicht.

So erstellen Sie Installationspakete:

1. Laden Sie die neuesten Versionen der folgenden Anwendungen und Plug-ins von der Kaspersky-Website herunter:
   - für Kaspersky Security für Windows Server: das Installationsprogramm und das Verwaltungs-Plug-in
   - für Kaspersky Endpoint Security für Linux: das Installationsprogramm, die Dateien zur Remote-Installation über Kaspersky Security Center und das Verwaltungs-Plug-in
2. Speichern Sie alle Dateien auf der Instanz (oder der virtuellen Maschine), auf welcher der Administrationsserver installiert ist.
3. Extrahieren Sie die Dateien aus allen Paketen.
4. Starten Sie Kaspersky Security Center.
5. Gehen Sie in der Konsolenstruktur zu **Erweitert** → **Remote-Installation** → **Installationspakete** und klicken Sie auf **Installationspaket erstellen**.
6. Wählen **Kaspersky-Installationspaket erstellen** aus.
7. Geben Sie den Namen für das Paket und den Pfad zum Installationsassistenten des Programms an:"<Order>\<Dateiname>.kud" und klicken Sie anschließend auf **Weiter**.
8. Lesen Sie die Endbenutzer-Lizenzvertrag und aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Bedingungen akzeptieren. Klicken Sie anschließend auf **Weiter**.

Das Installationspaket wird auf den Administrationsserver hochgeladen und ist in der Liste der Installationspakete verfügbar.

Die Konfiguration der Cloud-Umgebung wird verfügbar, sobald Sie die Installationspakete erstellt und die Verwaltungs-Plug-ins auf dem Administrationsserver installiert haben.

Eine Cloud-Umgebung konfigurieren

Um Kaspersky Security Center mithilfe des Assistenten zur Konfiguration der Cloud-Umgebung zu konfigurieren, müssen Sie über Folgendes verfügen:

- Spezifische Anmeldeinformationen für eine Cloud-Umgebung:
  - Eine IAM-Rolle, der die Berechtigung zur Abfrage des Cloud-Segments zugewiesen wurde, oder ein IAM-Benutzerkonto, dem die Berechtigung zur Abfrage des Cloud-Segments gewährt wurde (für das Arbeiten mit Amazon Web Services)
  - Eine Azure Anwendungs-ID, ein Kennwort und ein Abonnement (für das Arbeiten mit Microsoft Azure)
  - Eine Google-Client-E-Mail, Projekt-ID und privaten Schlüssel (für das Arbeiten mit Google Cloud)

- Installationspakete:
  - Administrationsagent für Windows
  - Administrationsagent für Linux
  - Kaspersky Endpoint Security für Linux
- Web-Plug-in für Kaspersky Endpoint Security für Linux
- Mindestens eines der folgenden:
  - Installationspaket und Web-Plug-in für Kaspersky Endpoint Security für Windows (empfohlen)
  - Installationspaket und Web-Plug-in für Kaspersky Security für Windows Server

Wenn Sie die Möglichkeiten zur Arbeit in der Cloud-Umgebung nicht nutzen möchten (z. B wenn Sie nur den Schutz von physischen Client-Geräten verwalten möchten), können Sie die Assistenten zur Konfiguration der Cloud-Umgebung schließen und den standardmäßigen Schnellstartassistenten für den Administrationsserver manuell starten.

Der Vorgang zur Konfiguration der Cloud-Umgebung wird automatisch bei der ersten Verbindung mit dem Administrationsserver über die Verwaltungskonsole gestartet, wenn Sie Kaspersky Security Center aus einem einsatzbereiten Abbild öffnen. Sie können den Assistenten zur Konfiguration der Cloud-Umgebung auch jederzeit manuell starten.

So starten Sie die den Assistenten zur Konfiguration der Cloud-Umgebung manuell:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **Alle Aufgaben → Konfigurieren der Cloud-Umgebung**.

Eine durchschnittliche Arbeitssitzung dauert etwa 15 Minuten.

Über den Assistenten zur Konfiguration der Cloud-Umgebung

Der Assistent zur Konfiguration der Cloud-Umgebung ermöglicht die Konfiguration von Kaspersky Security Center unter Berücksichtigung der Besonderheiten bei der Arbeit in einer Cloud-Umgebung.

Der Assistent erstellt folgende Objekte:

- Richtlinie für den Administrationsagenten mit den Standardeinstellungen
- Richtlinie für Kaspersky Endpoint Security für Linux
- Richtlinie für Kaspersky Security für Windows Server
- Administrationsgruppe für Instances und eine Regel zum automatischen Verschieben von Instances in diese Administrationsgruppe
- Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers
- Aufgaben zum Installation des Schutzes auf Geräten unter der Verwaltung von Linux und Windows

- Aufgaben für die einzelnen verwalteten Geräte:
  - Schnelle Schadsoftware-Untersuchung
  - Update-Download

Wenn Sie die Variante der Lizenzverwaltung gemäß dem Modell BYOL ausgewählt haben, aktiviert die Konfiguration der Cloud-Umgebung auch Kaspersky Security Center mithilfe einer Schlüsseldatei oder eines Aktivierungscodes und legt den Lizenzschlüssel oder den Aktivierungscode im Lizenzspeicher ab.

Schritt 1. Auswählen der Methode zur Programmaktivierung

Dieser Schritt wird nicht angezeigt, wenn Sie sich für eines der einsatzbereiten AMIs (im AWS Marketplace) oder für eine nutzungsbasierte monatlich abgerechnete SKU (im Azure Marketplace) angemeldet haben. In diesem Fall fährt der Assistent sofort mit dem nächsten Schritt fort. Für Google Cloud kann jedoch kein einsatzbereites AMI erworben werden.

Wenn Sie die Variante zur Lizenzverwaltung für Kaspersky Security Center gemäß dem BYOL-Schema ausgewählt haben, fordert der Assistent Sie auf, eine Programmaktivierungsmethode auszuwählen.

Aktivieren Sie das Programm mithilfe eines Aktivierungscodes (oder einer Schlüsseldatei) für Kaspersky Security for Virtualization oder Kaspersky Hybrid Cloud Security.

Sie können das Programm auf folgende Arten aktivieren:

- Aktivierungscode eingeben.

  Die Online-Aktivierung wird gestartet. Dieser Prozess umfasst die Verifizierung des festgelegten Aktivierungscodes sowie die Ausgabe und Aktivierung einer Schlüsseldatei.

- Schlüsseldatei angeben.

  Das Programm prüft die Schlüsseldatei und aktiviert sie, wenn die darin enthaltenen Informationen korrekten sind, oder schlägt vor, eine andere Schlüsseldatei anzugeben.

Kaspersky Security Center speichert den Lizenzschlüssel im Lizenzspeicher und kennzeichnet ihn als automatisch auf verwaltete Geräte zu verteilen.

Wenn Sie die Verbindung zur Instanz mithilfe des Microsoft Windows-Standardprogramms "Remotedesktopverbindung" (Remote Desktop Connection) oder eines ähnlichen Programms hergestellt haben, geben Sie in den Eigenschaften der Remote-Verbindung das Laufwerk des physischen Geräts an, das Sie zur Verbindung verwenden. So gewährleisten Sie den Zugriff von der Instanz auf die Dateien auf Ihrem realen Gerät und können die Schlüsseldatei auswählen.

Wenn Sie mit Kaspersky Security Center aus einem gebührenpflichtigen AMI oder mit einem nutzungsbasierten, monatlich verrechneten SKU arbeiten, können Sie keine Lizenzschlüssel oder Aktivierungscodes zum Lizenzspeicher hinzufügen.

Schritt 2. Auswählen der Cloud-Umgebung

Wählen Sie die Cloud-Umgebung aus, in der Sie Kaspersky Security Center AWS, Azure oder Google Cloud verteilen.

Schritt 3. Autorisieren in der Cloud-Umgebung

AWS

Wenn Sie AWS ausgewählt haben, legen Sie entweder fest, dass Sie über eine IAM-Rolle mit den erforderlichen Berechtigungen verfügen, oder Sie stellen den AWS IAM-Zugriffsschlüssel für Kaspersky Security Center bereit. Ohne IAM-Rolle bzw. AWS IAM-Zugriffsschlüssel ist die Abfrage von Cloud-Segmenten nicht möglich.

Passen Sie die folgenden Verbindungseinstellungen an, die im Weiteren für die Abfrage des Cloud-Segments verwendet werden:

- **Verbindungsname**

  Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

  Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

  Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

- **AWS IAM-Rolle verwenden**

  Wählen Sie diese Option aus, wenn Sie bereits eine IAM-Rolle für den Administrationsserver zur Verwendung mit AWS-Diensten erstellt haben.

- **AWS IAM-Benutzerkonto verwenden**

  Wählen Sie diese Variante aus, wenn Sie ein IAM-Benutzerkonto mit den erforderlichen Rechten besitzen und die ID des Schlüssels und den geheimen Schlüssel eingeben können.

  - **ID des Zugriffsschlüssels**

    ID des IAM-Zugriffsschlüssels (eine Abfolge von alphanumerischen Zeichen). Sie haben die Schlüssel-ID bei der Erstellung des IAM-Benutzerkontos erhalten.

    Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

  - **Geheimer Schlüssel**

    Geheimer Schlüssel, den Sie gemeinsam mit der ID des Zugriffsschlüssels erhalten haben, als Sie das IAM-Benutzerkonto erstellt haben.

    Die Zeichen des geheimen Schlüssels werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des geheimen Schlüssels begonnen haben, wird die Schaltfläche **Anzeigen** angezeigt. Klicken Sie auf diese Schaltfläche und halten Sie diese so lange wie nötig gedrückt, um die eingegebenen Zeichen anzuzeigen.

Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

Diese Verbindung wird in den Programmeinstellungen gespeichert. Mit der Konfiguration der Cloud-Umgebung können Sie nur einen einzigen AWS IAM-Zugriffsschlüssel erstellen. Nachfolgend können Sie auch weitere Verbindungen für die Verwaltung anderer Cloud-Segmente angeben.

Wenn Sie Programme mithilfe von Kaspersky Security Center auf Instances installieren möchten, muss Ihre IAM-Rolle (bzw. der IAM-Benutzer, dessen Benutzerkonto dem von Ihnen eingegebene Schlüssel entspricht) über die erforderlichen Berechtigungen verfügen.

Azure

Wenn Sie Azure ausgewählt haben, passen Sie die folgenden Verbindungseinstellungen an, die im Weiteren für die Abfrage des Cloud-Segments verwendet werden:

- **Verbindungsname**

  Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

  Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

  Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

- **Anwendungs-ID für Azure**

  Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

  Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

- **Azure-Abonnement-ID**

  Sie haben das Abonnement auf dem Azure-Portal erstellt.

- **Azure-App-Kennwort**

  Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

  Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

- **Name des Azure-Speicherkontos**

  Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

- **Zugriffsschlüssel für Azure-Speicher**

  Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Security Center erstellt haben.

  Sie finden den Schlüssel im Abschnitt "Übersicht über das Azure-Speicherkonto" im Unterabschnitt "Schlüssel".

Diese Verbindung wird in den Programmeinstellungen gespeichert.

Google Cloud

Wenn Sie Google Cloud ausgewählt haben, passen Sie die folgenden Verbindungseinstellungen an, die im Weiteren für die Abfrage des Cloud-Segments verwendet werden:

- **Verbindungsname**

  Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

  Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

  Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

- **Client-E-Mail**

  Client-E-Mail ist die E-Mail-Adresse, die Sie für Ihr Projekt bei Google Cloud registriert haben.

- **Projekt-ID**

  Projekt-ID ist die ID, die Sie erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben.

- **Privater Schlüssel**

  Privater Schlüssel ist die Zeichenfolge, die Sie als privaten Schlüssel erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben. Um Fehler zu vermeiden können Sie die Zeichenfolge kopieren und einfügen.

Diese Verbindung wird in den Programmeinstellungen gespeichert.

Schritt 4. Konfigurieren der Cloud-Synchronisation und Wählen weiterer Maßnahmen

In diesem Schritt wird die Abfrage von Cloud-Segmenten gestartet und eine spezielle Administrationsgruppe für Instances wird erstellt. Die bei der Abfrage gefundene Instances werden in diese Gruppe verschoben. Der Zeitplan für die Abfrage des Cloud-Segments kann hier angepasst werden (standardmäßig alle 5 Minuten).

Des Weiteren wird eine Regel für das automatische Verschieben **Synchronisierung mit Cloud** erstellt. Bei jedem nachfolgenden Scannen des Cloud-Netzwerks werden die gefundenen virtuellen Geräte in die entsprechende Untergruppe innerhalb der Gruppe **Verwaltete Geräte\Cloud** verschoben.

Auf der Seite **Synchronisation mit dem Cloud-Segment** können Sie die folgenden Einstellungen angeben:

- **Struktur der Administrationsgruppe mit dem Cloud-Segment synchronisieren**

  Wenn diese Option aktiviert ist, wird innerhalb der Gruppe **Verwaltete Geräte** automatisch die Gruppe **Cloud** erstellt und eine Gerätesuche in der Cloud ausgeführt. Die Instances und virtuellen Maschinen, die jeweils während der Untersuchung des Cloud-Netzwerks gefunden werden, werden in die Cloud-Gruppe verschoben. Die Struktur der Verwaltungsuntergruppen innerhalb dieser Gruppe stimmt mit der Struktur Ihres Cloud-Segments überein (in AWS werden Verfügbarkeitszone und Zuordnungsgruppen nicht in der Struktur dargestellt; in Azure werden Subnetze nicht in der Struktur dargestellt). Geräte, die nicht als Instances in der Cloud-Umgebung identifiziert werden, befinden sich in der Gruppe **Nicht zugeordnete Geräte**. Eine solche Gruppenstruktur ermöglicht, mithilfe der Aufgaben zur Gruppeninstallation Antiviren-Programme auf Instances zu installieren und verschiedene Richtlinien für verschiedene Gruppen anzupassen.

Wenn diese Option deaktiviert ist, wird auch die Gruppe **Cloud** erstellt und eine Gerätesuche in der Cloud wird gestartet; Untergruppen, die der Struktur des Cloud-Segments entsprechen, werden jedoch innerhalb der Gruppe nicht erstellt. Alle gefundenen Instances befinden sich in der **Cloud**-Administrationsgruppe und werden daher als einheitliche Liste angezeigt. Wenn während der Ausführung von Kaspersky Security Center eine Synchronisierung vorgenommen werden muss, können Sie die Eigenschaften der Regel **Synchronisierung mit Cloud** ändern und diese erzwingen. Durch das Erzwingen der Regel wird die Struktur der Gruppen innerhalb der Cloud-Gruppe neu angeordnet, sodass sie der Struktur Ihres Cloud-Segments entspricht.

Diese Option ist standardmäßig deaktiviert.

- **Schutz bereitstellen**

  Wenn diese Option ausgewählt ist, erstellt der Assistent eine Aufgabe zur Installation der Sicherheitsanwendungen auf den Instances. Nach dem Fertigstellen des Assistenten wird automatisch der Assistent für die Bereitstellung des Schutzes auf den Geräten in Ihren Cloud-Segmenten gestartet, und Sie können auf diesen Geräten den Administrationsagenten und die Sicherheitsanwendungen installieren.

  Kaspersky Security Center kann die Bereitstellung mit seinen nativen Instrumenten durchführen. Wenn Sie keine Berechtigung haben, um die Anwendungen auf den EC2-Instances oder auf virtuellen Azure-Maschinen zu installieren, können Sie die Aufgabe **Remote-Installation** manuell konfigurieren und ein Benutzerkonto mit den erforderlichen Berechtigungen angeben. In diesem Fall kann die Aufgabe "Remote-Installation" nicht für Geräte verwendet werden, die mit AWS API oder Azure gefunden wurden. Diese Aufgabe kann nur für Geräte verwendet werden, die mittels Abfrage des Active Directory, Abfrage der Windows-Domänen oder Durchsuchen der IP-Bereiche gefunden wurden.

  Wenn diese Option nicht ausgewählt ist, wird der Assistent für die Bereitstellung des Schutzes nicht gestartet und auch die Aufgaben zur Installation der Sicherheitsanwendungen auf Instances nicht erstellt. Sie können beide Aktionen später manuell durchführen.

Für Google Cloud können Sie die Bereitstellung ausschließlich mit den nativen Werkzeugen von Kaspersky Security Center durchführen. Wenn Sie Google Cloud ausgewählt haben, ist die Option **Schutz bereitstellen** nicht verfügbar.

Schritt 5. Konfigurieren von Kaspersky Security Network in der Cloud-Umgebung

Legen Sie die Einstellungen für die Übertragung von Informationen über die Ausführung von Kaspersky Security Center in die Wissensdatenbank von Kaspersky Security Network fest. Wählen Sie eine der folgenden Varianten aus:

- **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**

  Kaspersky Security Center und die verwalteten Programme, die auf Client-Geräten installiert sind, übertragen ihre Vorgangsdetails automatisch an Kaspersky Security Network. Die Zusammenarbeit mit Kaspersky Security Network gewährleistet ein schnelleres Datenbanken-Update mit Daten über Viren und Bedrohungen, wodurch die Reaktionsgeschwindigkeit auf neue Sicherheitsgefährdungen erhöht wird.

- **Ich lehne die Nutzungsbedingungen für Kaspersky Security Network ab**

  Kaspersky Security Center und verwaltete Programme senden keine Informationen an Kaspersky Security Network.

  Wenn Sie diese Option auswählen, wird die Verwendung von Kaspersky Security Network deaktiviert.

Kaspersky empfiehlt die Teilnahme an Kaspersky Security Network.

Schritt 6. Konfigurieren von E-Mail-Benachrichtigungen in der Cloud-Umgebung

In diesem Fenster können Sie Einstellungen für den Versand von Benachrichtigungen über Ereignisse anpassen, die bei der Ausführung von Kaspersky-Anwendungen auf den virtuellen Client-Geräten registriert werden. Diese Einstellungen werden in den Richtlinien für die Anwendungen als Standardwerte verwendet.

Folgende Einstellungen für den Versand von Benachrichtigungen über auftretende Ereignisse der Programme von Kaspersky können angepasst werden:

- **Empfänger (E-Mail-Adressen)**

  E-Mail-Adressen des Nutzers, an die das Programm Benachrichtigungen versenden soll. Sie können eine oder mehrere Adressen angeben. Geben Sie mehrere Adressen durch Semikolon getrennt an.

- **SMTP-Server**

  Adresse oder Adressen der Mail-Server Ihres Unternehmens.

  Geben Sie mehrere Adressen durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

  - IPv4- oder IPv6-Adresse
  - Windows-Netzwerkname (NetBIOS-Name) des Geräts
  - DNS-Name des SMTP-Servers

- **Port des SMTP-Servers**

  Kommunikationsportnummer des SMTP-Servers Wenn Sie mehrere SMTP-Server verwenden, wird die Verbindung zu diesen über den angegebenen Kommunikationsport hergestellt. Standardmäßig wird Portnummer 25 verwendet.

- **ESMTP-Authentifizierung verwenden**

  Aktivierung der Unterstützung von ESMTP-Authentifizierung. Nach der Aktivierung des Kontrollkästchens in den Feldern **Benutzername** und **Kennwort** können die Einstellungen für ESMTP-Authentifizierung angeben werden. Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

Sie können die festgelegten Versandeinstellungen der E-Mail-Benachrichtigungen mithilfe der Schaltfläche **Testnachricht senden** prüfen. Wenn die Testnachricht erfolgreich an die Adressen zugestellt wurde, die im Feld **Empfänger (E-Mail-Adressen)** angegeben sind, sind die Einstellungen richtig konfiguriert.

Schritt 7. Erstellen einer Erstkonfiguration des Schutzes für die Cloud-Umgebung

In diesem Schritt erstellt Kaspersky Security Center automatisch die Richtlinien und die Aufgaben. Im Fenster **Erstkonfiguration des Schutzes anlegen** wird eine Liste der vom Programm erstellten Richtlinien und Aufgaben angezeigt.

Wenn Sie ein RDS-Datenbank in der AWS-Cloud-Umgebung verwenden, müssen Sie ein IAM-Zugriffsschlüsselpaar für Kaspersky Security Center bereitstellen, wenn die Aufgabe zum Anlegen eines Backups des Administrationsservers erstellt wird. Füllen Sie in diesem Fall die folgenden Felder aus:

- **Name des S3-Buckets**

  Name des S3-Buckets, den Sie für das Backup erstellt haben.

- **ID des Zugriffsschlüssels**

  Sie haben die Schlüssel-ID (Abfolge von alphanumerischen Zeichen) erhalten, als Sie das IAM-Benutzerkonto erstellt haben, um mit der Speicher-Instanz des S3-Buckets zu arbeiten.

  Dieses Feld ist verfügbar, wenn Sie RDS-Datenbank auf einem S3-Bucket ausgewählt haben.

- **Geheimer Schlüssel**

  Geheimer Schlüssel, den Sie gemeinsam mit der ID des Zugriffsschlüssels erhalten haben, als Sie das IAM-Benutzerkonto erstellt haben.

  Die Zeichen des geheimen Schlüssels werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des geheimen Schlüssels begonnen haben, wird die Schaltfläche **Anzeigen** angezeigt. Klicken Sie auf diese Schaltfläche und halten Sie diese so lange wie nötig gedrückt, um die eingegebenen Zeichen anzuzeigen.

  Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

Wenn Sie ein Azure SQL-Datenbank in der Azure-Cloud-Umgebung verwenden, müssen Sie Informationen zu Ihrem Azure SQL Server für Kaspersky Security Center bereitstellen, wenn die Aufgabe zur Sicherung des Administrationsservers erstellt wird. Füllen Sie in diesem Fall die folgenden Felder aus:

- **Name des Azure-Speicherkontos**

  Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

- **Azure-Abonnement-ID**

  Sie haben das Abonnement auf dem Azure-Portal erstellt.

- **Azure-App-Kennwort**

  Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

  Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

- **Anwendungs-ID für Azure**

  Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

  Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

- **Name des Azure SQL-Servers**

  Der Name und die Gruppe der Ressourcen sind in den Eigenschaften Ihres Azure SQL-Servers verfügbar.

- **Azure SQL-Serverressourcengruppe**

  Der Name und die Gruppe der Ressourcen sind in den Eigenschaften Ihres Azure SQL-Servers verfügbar.

- **Zugriffsschlüssel für Azure-Speicher**

  Verfügbar in den Eigenschaften Ihres Speicherkontos im Abschnitt "Zugriffsschlüssel". Sie können einen der Schlüssel (Schlüssel1 oder Schlüssel2) verwenden.

Wenn Sie den Administrationsserver in der Google Cloud bereitstellen, müssen Sie einen Ordner auswählen, in dem die Backup-Kopien gespeichert werden. Wählen Sie einen Ordner auf Ihrem lokalen Gerät oder einen Ordner auf einer Instanz einer virtuellen Maschine aus.

Die Schaltfläche **Weiter** wird verfügbar, sobald alle für die minimale Konfiguration des Schutzes erforderlichen Richtlinien und Aufgaben erstellt sind.

Wenn ein Gerät, auf dem die Aufgaben ausgeführt werden sollen, für den Administrationsserver nicht sichtbar ist, dann werden die Aufgaben erst gestartet, wenn die Instance sichtbar wird. Wenn Sie eine neue EC2-Instance oder eine neue virtuelle Azure-Maschine erstellen, kann es eine Weile dauern, bevor die Instance für den Administrationsserver sichtbar wird. Wenn Sie möchten, dass der Administrationsagent und die Sicherheitsanwendungen auf allen neu erstellten Instances so rasch wie möglich installiert werden, stellen Sie sicher. dass die Option **Übersprungene Aufgaben starten** für die Aufgaben **Remote-Installation des Programms** aktiviert ist. Anderenfalls erhält eine neu installierte Instance/virtuelle Maschine den Administrationsagenten und die Sicherheitsanwendungen erst, wenn die Aufgabe gemäß ihrem Zeitplan gestartet wird.

Schritt 8. Auswählen der auszuführenden Maßnahme, wenn das Betriebssystem während der Installation einen Neustart erfordert (für Cloud-Umgebung)

Wenn Sie zuvor **Schutz bereitstellen** ausgewählt haben, müssen Sie Aktionen für den Fall festlegen, dass ein Zielgerät neu gestartet werden soll. Wenn Sie die Option **Schutz bereitstellen** nicht aktiviert haben, wird dieser Schritt übersprungen.

Bestimmen Sie, ob Instances erneut geladen werden sollen, wenn im Verlauf der Programminstallation ein Neustart des Geräte-Betriebssystems erforderlich ist:

- **Gerät nicht neu starten**

  Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung nicht neu gestartet.

- **Gerät neu starten**

  Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung neu gestartet.

Wenn Sie auf allen Instances vor dem Neustart das Beenden der Anwendungen in blockierten Sitzungen erzwingen möchten, aktivieren Sie das Kontrollkästchen **Beenden von Programmen in blockierten Sitzungen erzwingen**. Wenn das Fähnchen nicht aktiviert ist, müssen alle Programme, die auf blockierten Instances ausgeführt werden, manuell geschlossen werden.

Schritt 9. Empfangen von Updates durch den Administrationsserver

In diesem Schritt wird der Fortschritt des Downloads von Updates angezeigt, die für die korrekte Arbeit des Administrationsservers erforderlich sind. Sie können auf **Weiter** klicken, ohne den Abschluss des Downloads abzuwarten, und zur letzten Seite des Assistenten wechseln.

Daraufhin wird der Assistent abgeschlossen.

Überprüfen der Konfiguration

Um zu überprüfen, ob Kaspersky Security Center 15.1 korrekt für die Arbeit in der Cloud-Umgebung konfiguriert ist, gehen Sie wie folgt vor:

1. Starten Sie Kaspersky Security Center und vergewissern Sie sich, dass Sie sich mithilfe der Verwaltungskonsole mit dem Administrationsserver verbinden können.

2. Wählen Sie in der Konsolenstruktur den Punkt **Verwaltete Geräte\Cloud** aus.

3. Wenn Sie Untergruppe innerhalb der Gruppe **Verwaltete Geräte\Cloud** anzeigen, vergewissern Sie sich, dass auf der Registerkarte **Geräte** alle Geräte dieser Untergruppe angezeigt werden.

   Wenn die Geräte nicht angezeigt werden, können Sie die zugehörigen Cloud-Segmente manuell abfragen, um sie zu finden.

4. Stellen Sie sicher, dass auf der Registerkarte **Richtlinien** folgende Programme aktive Richtlinien besitzen:

   - Kaspersky Security Center Administrationsagent
   - Kaspersky Security für Windows Server
   - Kaspersky Endpoint Security für Linux

   Wenn sie nicht aufgelistet sind, können Sie diese manuell erstellen.

5. Stellen Sie sicher, dass auf der Registerkarte **Aufgaben** die folgenden Aufgaben vorhanden sind:

   - **Backup der Daten des Administrationsservers anlegen**
   - **Update-Aufgabe für Windows Server**
   - **Wartung des Administrationsservers**
   - **Download von Updates in die Datenverwaltung des Administrationsservers**
   - **Suche nach Schwachstellen und erforderlichen Updates**
   - **Schutz für Windows installieren**
   - **Schutz für Linux installieren**
   - **Schnelle Untersuchung für Windows Server**
   - **Schnelle Untersuchung**
   - **Updates für Linux installieren**

   Wenn sie nicht aufgelistet sind, können Sie diese manuell erstellen.

Kaspersky Security Center 15.1 ist korrekt für die Arbeit in einer Cloud-Umgebung konfiguriert.

Gruppe der Cloud-Geräte

Sie können Cloud-Geräte verwalten, indem Sie diese in Gruppen zusammenfassen. Während der Phase der Erstkonfiguration von Kaspersky Security Center wird die Administrationsgruppe **Verwaltete Geräte\Cloud** standardmäßig erstellt und die während einer Abfrage im Netzwerk gefunden Cloud-Geräte werden in diese Gruppe verschoben.

Wenn Sie die Option **Struktur der Administrationsgruppe mit dem Cloud-Segment synchronisieren** gewählt haben, während Sie die Synchronisierung konfiguriert haben, entspricht die Struktur der Untergruppen in dieser Administrationsgruppe der Struktur Ihrer Cloud-Segmente (In AWS werden jedoch Verfügbarkeitszonen und Zuordnungsgruppen nicht in der Struktur dargestellt; in Microsoft Azure werden Subnetze nicht in der Struktur dargestellt.). Leere Untergruppen innerhalb der Gruppe, die bei der Abfrage im Netzwerk gefunden werden, werden automatisch gelöscht.

Sie können auch selbständig Administrationsgruppen erstellen, in denen alle oder eine Reihe von Geräten zusammengefasst sind.

Die Gruppe **Verwaltete Geräte\Cloud** erbt standardmäßig die Richtlinien und Aufgaben der Gruppe **Verwaltete Geräte**. Sie können die Einstellungen ändern, wenn in den Eigenschaften der Einstellungen der entsprechenden Richtlinien und Aufgaben die Kontrollkästchen **Bearbeitung erlaubt** aktiviert sind.

Abfrage des Netzwerksegments

Der Administrationsserver erhält Daten über die Netzwerkstruktur und deren Geräte anhand von regelmäßigen Abfragen der Cloud-Segmente durch die Tools der AWS-API, Azure-API oder Google-API. Auf Grundlage der empfangenen Daten aktualisiert Kaspersky Security Center den Inhalt der Ordner **Nicht zugeordnete Geräte** und **Verwaltete Geräte**. Wenn Sie in einem Firmennetzwerk das automatische Verschieben von Geräten in Administrationsgruppen eingerichtet haben, werden die im Netzwerk gefundenen Geräte in Administrationsgruppen aufgenommen.

Zur Abfrage von Cloud-Segmenten durch den Administrationsserver sind Rechte erforderlich, die mit einer IAM-Rolle oder einem IAM-Benutzerkonto (in AWS), einer Anwendungs-ID und Kennwort (in Azure) oder mit Client-E-Mail, Projekt-ID und privaten Schlüssel (in Google) gewährt werden.

Sie können Verbindungen, hinzufügen und entfernen sowie für jedes Cloud-Segment einen Zeitplan für die Abfrage einrichten.

Hinzufügen von Verbindungen für die Abfrage von Cloud-Segmenten

Um die Verbindung für die Abfrage von Cloud-Segmenten zur Liste der verfügbaren Verbindungen hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Knoten **Gerätesuche** → **Cloud** aus.

2. Klicken Sie im Arbeitsbereich des Fensters auf **Abfrageeinstellungen anpassen**.

   Ein Eigenschaftenfenster mit einer Liste der für die Abfrage der Cloud-Segmente verwendeten Verbindungen wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Verbindung** wird geöffnet.

4. Geben Sie den Namen der Cloud-Umgebung für die Verbindung an, die im Weiteren für die Abfrage des Cloud-Segments verwendet werden:

   Cloud-Umgebung

   Die Umgebung, in der sich die EC2-Instances oder virtuellen Maschinen befinden. Mögliche Umgebungen sind: Amazon Web Services (AWS), Microsoft Azure oder Google Cloud.

   Wenn Sie AWS ausgewählt haben, geben Sie die folgenden Einstellungen an:

   - **Verbindungsname**

     Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

     Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

     Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

   - **AWS IAM-Rolle verwenden**

     Wählen Sie diese Option aus, wenn Sie bereits eine IAM-Rolle für den Administrationsserver zur Verwendung mit AWS-Diensten erstellt haben.

   - **AWS IAM-Benutzerkonto verwenden**

     Wählen Sie diese Variante aus, wenn Sie ein IAM-Benutzerkonto mit den erforderlichen Rechten besitzen und die ID des Schlüssels und den geheimen Schlüssel eingeben können.

     - **ID des Zugriffsschlüssels**

       ID des IAM-Zugriffsschlüssels (eine Abfolge von alphanumerischen Zeichen). Sie haben die Schlüssel-ID bei der Erstellung des IAM-Benutzerkontos erhalten.

       Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

     - **Geheimer Schlüssel**

       Geheimer Schlüssel, den Sie gemeinsam mit der ID des Zugriffsschlüssels erhalten haben, als Sie das IAM-Benutzerkonto erstellt haben.

       Die Zeichen des geheimen Schlüssels werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des geheimen Schlüssels begonnen haben, wird die Schaltfläche **Anzeigen** angezeigt. Klicken Sie auf diese Schaltfläche und halten Sie diese so lange wie nötig gedrückt, um die eingegebenen Zeichen anzuzeigen.

       Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

   Mit dem Assistenten zur Konfiguration der Cloud-Umgebung kann nur ein einziger AWS IAM-Zugriffsschlüssel angegeben werden. Nachfolgend können Sie auch weitere Verbindungen für die Verwaltung anderer Cloud-Segmente angeben.

Wenn Sie Azure ausgewählt haben, geben Sie die folgenden Einstellungen an:

- **Verbindungsname**

  Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

  Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

  Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

- **Anwendungs-ID für Azure**

  Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

  Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

- **Azure-Abonnement-ID**

  Sie haben das Abonnement auf dem Azure-Portal erstellt.

- **Azure-App-Kennwort**

  Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

  Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

- **Name des Azure-Speicherkontos**

  Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

- **Zugriffsschlüssel für Azure-Speicher**

  Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Security Center erstellt haben.

  Sie finden den Schlüssel im Abschnitt "Übersicht über das Azure-Speicherkonto" im Unterabschnitt "Schlüssel".

Wenn Sie Google Cloud ausgewählt haben, geben Sie die folgenden Einstellungen an:

- **Verbindungsname**

  Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

  Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

  Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

- **Client-E-Mail**

  Client-E-Mail ist die E-Mail-Adresse, die Sie für Ihr Projekt bei Google Cloud registriert haben.

- **Projekt-ID**

  Projekt-ID ist die ID, die Sie erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben.

- **Privater Schlüssel**

  Privater Schlüssel ist die Zeichenfolge, die Sie als privaten Schlüssel erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben. Um Fehler zu vermeiden können Sie die Zeichenfolge kopieren und einfügen.

5. Klicken Sie gegebenenfalls auf **Abfragezeitplan festlegen** und ändern Sie die Standardeinstellungen.

Die Verbindung wird in den Programmeinstellungen gespeichert.

Nach der ersten Abfrage des neuen Cloud-Segments erscheint in der Administrationsgruppe **Verwaltete Geräte\Cloud** eine Untergruppe, die diesem Segment entspricht.

Wenn die von Ihnen angegebenen Benutzerdaten falsch sind, werden bei der Abfrage des Cloud-Segments keine Instances gefunden und in der Administrationsgruppe **Verwaltete Geräte\Cloud** wird keine neue Untergruppe angezeigt.

Entfernen von Verbindungen für die Abfrage von Cloud-Segmenten

Wenn Sie ein bestimmtes Cloud-Segment nicht mehr abfragen müssen, können Sie die Verbindung, die diesem Segment entspricht, aus der Liste der verfügbaren Verbindungen löschen. Sie können die Verbindung auch löschen, wenn z. B. die Berechtigung zur Abfrage des Cloud-Segments an einen anderen AWS IAM-Benutzer mit anderem Schlüssel übertragen wurde.

Gehen Sie folgendermaßen vor, um eine Verbindung zu löschen:

1. Wählen Sie im Konsolenbaum den Knoten **Gerätesuche** → **Cloud** aus.
2. Wählen Sie im Arbeitsbereich des Fensters den Punkt **Abfrageeinstellungen anpassen** aus.

   Ein Fenster mit einer Liste der für die Abfrage der Cloud-Segmente verwendeten Verbindungen wird angezeigt.
3. Markieren Sie die Verbindung, die Sie löschen möchten, und klicken Sie im rechten Fensterbereich auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **OK**, um die Auswahl zu bestätigen.

Wenn Sie eine Verbindung aus der Liste der verfügbaren Verbindungen löschen, werden die Geräte, die sich in den entsprechenden Segmenten befinden, automatisch aus den entsprechenden Administrationsgruppen entfernt.

Abfragezeitplan anpassen

Die Abfrage des Cloud-Segments erfolgt nach Zeitplan. Sie können das Intervall festlegen, in dem die Abfrage durchgeführt wird.

Das Intervall für die Abfrage wird in den Einstellungen zur Konfiguration der Cloud-Umgebung automatisch auf 5 Minuten festgelegt. Sie können diesen Wert jederzeit ändern und einen anderen Zeitplan festlegen. Es wird jedoch nicht empfohlen, die Einstellungen der Abfrage so anzupassen, dass sie öfter als alle 5 Minuten durchgeführt wird, da dies zu Fehlern in der Ausführung der API führen kann.

Gehen Sie folgendermaßen vor, um den Abfragezeitplan für das Cloud-Segment anzupassen:

1. Wählen Sie im Konsolenbaum den Knoten **Gerätesuche** → **Cloud** aus.
2. Klicken Sie im Arbeitsbereich auf **Abfrageeinstellungen anpassen**.

   Das Cloud-Eigenschaftenfenster wird geöffnet.
3. Wählen Sie in der Liste die gewünschte Verbindung aus und klicken Sie auf **Eigenschaften**.

   Das Eigenschaftenfenster der Verbindung wird geöffnet.
4. Klicken Sie im Eigenschaftenfenster auf den Link **Abfragezeitplan festlegen**.

   Das Fenster **Zeitplan** wird angezeigt.
5. Passen Sie die folgenden Einstellungen an:

   - **Start nach Zeitplan**

     Varianten für den Zeitplan der Abfrage:

     - **Alle n Tage**

       Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

       Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

     - **Alle n Minuten**

       Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

       Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

     - **Nach Wochentagen**

       Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

       Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

     - **Monatlich, an angegebenen Tagen der gewählten Wochen**

       Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

       Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

   - **Übersprungene Aufgaben starten**

     Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

     Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

     Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

Diese Option ist standardmäßig aktiviert.

6. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Der Abfragezeitplan wurde konfiguriert und gespeichert.

Installation von Programmen auf Geräten in einer Cloud-Umgebung

Sie können auf den Geräten in Cloud-Umgebung folgende Kaspersky-Anwendungen installieren: Kaspersky Security für Windows Server (für Windows-Geräte) und Kaspersky Endpoint Security für Linux (für Linux-Geräte).

Die Client-Geräte, auf denen Sie den Schutz installieren möchten, müssen die Anforderungen erfüllen, die für die Arbeit von Kaspersky Security Center in der Cloud-Umgebung festgelegt sind. Sie müssen über eine gültige Lizenz verfügen, um Anwendungen auf AWS-Instances, virtuellen Microsoft Azure-Maschinen oder Instanzen virtueller Maschinen von Google Cloud zu installieren.

Kaspersky Security Center 15.1 unterstützt die folgenden Szenarien:

- Ein Client-Gerät wird mittels API gefunden; die Installation erfolgt mittels API. Dieses Szenario wird für die Cloud-Umgebungen von AWS und Azure unterstützt.
- Ein Client-Gerät wird mittels Abfrage des Active Directory, Abfrage von Windows-Domänen oder Durchsuchen der IP-Bereiche gefunden; die Installation erfolgt über Kaspersky Security Center.
- Ein Client-Gerät wird mittels Google-API gefunden; die Installation erfolgt mittels Kaspersky Security Center. Für Google Cloud wird nur dieses Szenario unterstützt.

Es werden keine anderen Installationsmethoden unterstützt.

Verwenden Sie die Installationspakete, um die Programme auf den virtuellen Geräten zu installieren.

Um mithilfe von AWS API oder Azure API eine Aufgabe zur Remote-Installation des Programms auf Instances zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.
3. Wählen Sie auf der Seite **Aufgabentyp auswählen** den Aufgabentyp **Remote-Installation des Programms** aus.
4. Wählen Sie auf der Seite **Geräte auswählen** die gewünschten Geräte aus der Gruppe **Verwaltete Geräte\Cloud** aus.

5. Wenn auf den Geräten, auf denen Sie das Programm installieren möchten, noch kein Administrationsagent installiert ist, wählen Sie auf der Seite **Benutzerkonto für die Ausführung der Aufgabe auswählen** die Option **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)** aus und klicken Sie im rechten Fensterbereich auf **Hinzufügen**. Wählen Sie im sich öffnenden Menü Folgendes aus:

   - **Cloud-Benutzerkonto**

     Wählen Sie diese Option aus, wenn Sie Programme auf den Instances in der AWS- oder Azure-Umgebung installieren möchten und über einen AWS IAM-Zugriffsschlüssel mit den erforderlichen Berechtigungen, jedoch über keine IAM-Rolle verfügen. Wählen Sie diese Option auch aus, wenn Sie Programme auf Geräten in der Azure-Umgebung installieren möchten.

     Stellen Sie im nächsten Fenster für Kaspersky Security Center die Anmeldedaten bereit, die zur Installation von Programmen auf die gewünschten Geräte berechtigt.

     Wählen Sie die Cloud-Umgebung aus: AWS oder Azure.

     Geben Sie im Feld **Benutzerkonto-Name** einen Namen für das Benutzerkonto für diese Anmeldedaten ein. Dieser Name wird in der Liste der Benutzerkonten zur Ausführung der Aufgabe angezeigt.

     Wenn Sie AWS ausgewählt haben, geben Sie in den Feldern **ID des Zugriffsschlüssels** und **Geheimer Schlüssel** die Anmeldedaten für das IAM-Benutzerkonto an, das über die Berechtigungen zur Installation von Programmen auf den festgelegten Geräten verfügt.

     Wenn Sie Azure ausgewählt haben, geben Sie in den Feldern **Azure-Abonnement-ID** und **Azure-App-Kennwort** die Anmeldedaten für das Azure-Benutzerkonto an, das über die Berechtigungen zur Installation von Programmen auf den festgelegten Geräten verfügt.

     Wenn Sie ungültige Anmeldedaten festlegen, wird die Aufgabe zur Remote-Installation auf den Geräten, für die sie geplant ist, mit einem Fehler beendet.

   - **Benutzerkonto**

     Wählen Sie diese Option für Instances unter Windows aus, wenn Sie nicht vorhaben, das Programm mithilfe von AWS oder Azure API-Instrumenten zu installieren. Vergewissern Sie sich in diesem Fall, dass die Geräte in Ihrem Cloud-Segment den erforderlichen Bedingungen entsprechen. Kaspersky Security Center führt die Installation der Programme mit eigenen Mitteln ohne Verwendung von AWS API oder Azure API durch.

     Wenn Sie ungültige Daten festlegen, wird die Aufgabe zur Remote-Installation auf den Geräten, für die sie geplant ist, mit einem Fehler beendet.

   - **IAM-Rolle**

     Wählen Sie diese Option aus, wenn Sie Programme auf den Instances in der AWS-Umgebung installieren möchten und über eine IAM-Rolle mit den erforderlichen Berechtigungen verfügen.

     Wenn Sie diese Option auswählen, jedoch nicht über eine IAM-Rolle mit den erforderlichen Berechtigungen verfügen, wird die Aufgabe zur Remote-Installation auf den Geräten, für die sie geplant ist, mit einem Fehler beendet.

   - **SSH-Zertifikat**

     Wählen Sie diese Option für Instances unter Linux aus, wenn Sie nicht vorhaben, das Programm mithilfe von AWS API- oder Azure API-Instrumenten zu installieren. Vergewissern Sie sich in diesem Fall, dass die Geräte in Ihrem Cloud-Segment den erforderlichen Bedingungen entsprechen. Kaspersky Security Center führt die Installation der Programme mit eigenen Mitteln ohne Verwendung von AWS API oder Azure API durch.

     Um den privaten Schlüssel des SSH-Zertifikats anzugeben, können Sie ihn mit dem Tool "ssh-keygen" generieren. Beachten Sie, dass die Kaspersky Security Center das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" die Option `-m PEM` hinzu. Beispielsweise:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<Benutzer-E-Mail>"
```

Sie können mehrere Anmeldedaten hinzufügen, indem Sie mehrmals auf **Hinzufügen** klicken. Wenn für unterschiedliche Cloud-Segmente unterschiedliche Anmeldedaten benötigt werden, stellen Sie die Anmeldedaten für alle Segmente bereit.

Nachdem der Assistent abgeschlossen ist, wird die Aufgabe zur Remote-Installation des Programms wird in der Aufgabenliste im Arbeitsbereich des Ordners **Aufgaben** angezeigt.

In Microsoft Azure kann die Remote-Installation von Sicherheitsanwendungen auf einer virtuellen Maschine dazu führen, dass die auf dieser virtuellen Maschine installierte Custom Script Extension gelöscht wird.

Eigenschaften von Cloud-Geräten anzeigen

Um die Eigenschaften eines Cloud-Gerätes anzuzeigen:

1. Wählen Sie in der Konsolenstruktur im Knoten **Gerätesuche** → **Cloud** den Knoten aus, der jener Gruppe entspricht, in welcher sich die betreffende Instanz befindet.

   Wenn Sie nicht wissen, in welcher Gruppe sich das gewünschte virtuelle Gerät befindet, verwenden Sie die Suchfunktion:

   a. Klicken Sie mit der rechten Maustaste auf den Namen des Knotens **Verwaltete Geräte** → **Cloud**, und wählen Sie anschließend die Option **Suchen** im Kontextmenü aus.

   b. Führen Sie im nächsten Fenster eine Suche durch.

      Wenn ein Gerät existiert, das den eingegebenen Kriterien entspricht, werden sein Name und die entsprechenden Informationen im unteren Bereich des Fensters angezeigt.

2. Klicken Sie mit der rechten Maustaste auf den Namen des gewünschten Knotens. Wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.

   Im folgenden Fenster werden die Eigenschaften des Objektes angezeigt.

   Der Abschnitt **Systeminformationen** → **Allgemeine Systeminformationen** enthält die Eigenschaften, die für Geräte in der Cloud-Umgebung festgelegt sind:

   - **Gerätesuche mithilfe von API** (**AWS**, **Azure** oder **Google Cloud**; wenn das Gerät mit den API-Tools nicht erkannt werden kann, wird der Wert **Nein** angezeigt).
   - **Cloud-Region**.
   - **Cloud VPC** (nur für AWS- und Google Cloud-Geräte).
   - **Availability Zone (Verfügbarkeitszone) der Cloud** (nur für AWS- und Google Cloud-Geräte).
   - **Subnetz der Cloud**.
   - **Platzierungsgruppe in der Cloud** (Dieses Element wird nur angezeigt, wenn die Instance zu einer Platzierungsgruppe gehört - andernfalls wird es nicht angezeigt).

Sie können auf die Schaltfläche **In Datei exportieren** klicken, um diese Informationen in eine csv- oder txt-Datei zu exportieren.

Synchronisierung mit der Cloud

Im Rahmen der Konfiguration der Cloud-Umgebung wird die Regel zur Synchronisierung mit Cloud automatisch erstellt. Die Regel ermöglicht eine automatische Verschiebung von Instances, die bei den einzelnen Abfragen gefunden werden, aus der Gruppe **Nicht zugeordnete Geräte** in die Gruppe **Verwaltete Geräte\Cloud**, damit die Instance für eine zentralisierte Verwaltung verfügbar ist. Standardmäßig wird die Regel nach der Erstellung aktiviert. Sie können die Regel jederzeit deaktivieren, ändern oder erzwingen.

Um die Eigenschaften der Regel Synchronisierung mit Cloud zu ändern bzw. zu erzwingen, gehen Sie wie folgt vor:

1. Klicken Sie im Konsolenbaum mit der rechten Maustaste auf den Namen des Knotens **Gerätesuche**.
2. Wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.
3. Wählen Sie im angezeigten Fenster **Eigenschaften** im Bereich **Abschnitte** den Punkt **Geräte verschieben** aus.
4. Wählen Sie im Arbeitsbereich in der Liste der Regeln für das Verschieben von Geräten die Regel **Synchronisierung mit Cloud** aus und klicken Sie unten im Fenster auf die Schaltfläche **Eigenschaften**.

   Das Eigenschaftenfenster der Regel wird geöffnet.
5. Legen Sie bei Bedarf die folgenden Einstellungen im Einstellungsblock **Cloud-Segmente** fest:

   - **Gerät befindet sich in einem Cloud-Segment**

     Die Regel wird nur auf Geräte verteilt, die sich im ausgewählten Cloud-Segment befinden. Andernfalls wird die Regel auf alle gefundenen Geräte angewendet.

     Diese Variante ist standardmäßig ausgewählt.

     - **Inklusive untergeordneter Objekte**

       Die Regel wird auf alle Geräten im ausgewählten Segment und in allen untergeordneten Cloud-Abschnitten verteilt. Anderenfalls wird die Regel nur auf Geräte verteilt, die sich im Stammsegment befinden.

       Diese Variante ist standardmäßig ausgewählt.

     - **Geräte aus untergeordneten Objekten in entsprechende Gruppen verschieben**

       Wenn diese Option aktiviert ist, werden Geräte aus untergeordneten Objekten automatisch in die Untergruppen verschoben, die ihrer Struktur entsprechen.

       Wenn diese Option deaktiviert ist, werden Geräte aus untergeordneten Objekten automatisch ohne weitere Aufteilung in den Stamm der Cloud-Untergruppe verschoben.

       Diese Option ist standardmäßig aktiviert.

       - **Untergruppen erstellen, die Containern von neu gefundenen Geräten entsprechen**

         Wenn diese Option aktiviert ist und in der Struktur der Gruppe **Verwaltete Geräte\Cloud** keine Untergruppen vorhanden sind, die jenem Abschnitt entsprechen würden, in dem sich das Gerät befindet, werden die entsprechenden Untergruppen von Kaspersky Security Center erstellt. Wird zum Beispiel ein neues Subnetz während der Gerätesuche gefunden, wird eine neue Gruppe mit dem gleichen Namen in der Gruppe **Verwaltete Geräte\Cloud** erstellt.

Wenn diese Option deaktiviert ist, erstellt Kaspersky Security Center keine neuen Untergruppen. Wenn zum Beispiel ein neues Subnetz während der Netzwerkabfrage gefunden wird, wird eine neue Gruppe mit dem gleichen Namen in der Gruppe **Verwaltete Geräte\Cloud** erstellt und die im Subnetz enthaltenen Geräte werden in die Gruppe **Verwaltete Geräte\Cloud** verschoben.

Diese Option ist standardmäßig aktiviert.

- **Untergruppen ohne Entsprechungen in Cloud-Segmenten löschen**

  Wenn diese Option aktiviert ist, löscht das Programm alle Untergruppen, die keinen der existierenden Cloud-Objekten entsprechen, aus der Cloud-Gruppe.

  Wenn diese Option deaktiviert ist, werden Untergruppen, die keinem der existierenden Cloud-Objekten entsprechen, beibehalten.

  Diese Option ist standardmäßig aktiviert.

Wenn Sie während der Konfiguration der Cloud-Umgebung die Option **Synchronisierung mit Cloud** aktiviert haben, wurde die Regel zur Synchronisierung mit der Cloud erstellt, in welcher die Kontrollkästchen **Untergruppen erstellen, die Containern von neu gefundenen Geräten entsprechen** und **Untergruppen ohne Entsprechungen in Cloud-Segmenten löschen** aktiviert sind.

Wenn Sie die Option **Synchronisierung mit Cloud** nicht aktiviert haben, wird die Regel Synchronisierung mit Cloud erstellt, wobei diese Option deaktiviert (nicht ausgewählt) ist. Wenn Sie bei der Verwendung von Kaspersky Security Center beschließen, dass die Struktur der Untergruppen innerhalb der Untergruppe **Verwaltete Geräte\Cloud** der Struktur der Cloud-Segmente entsprechen soll, aktivieren Sie in den Eigenschaften der Regel die Optionen **Untergruppen erstellen, die Containern von neu gefundenen Geräten entsprechen** und **Untergruppen ohne Entsprechungen in Cloud-Segmenten löschen** und erzwingen Sie dann die Regel.

6. Wählen Sie in der Dropdown-Liste **Gefunden mithilfe von API** einen Wert aus:
   - **AWS**. Das Gerät wird mithilfe der AWS-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von AWS.
   - **Azure**. Das Gerät wird mithilfe der Azure-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Azure.
   - **Google Cloud.** Das Gerät wird mithilfe der Google-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Google.
   - **Nein**. Das Gerät wird nicht mithilfe der AWS-, Azure- oder Google-API gefunden. Das heißt, es befindet sich entweder außerhalb der Cloud-Umgebung oder es befindet sich in der Cloud-Umgebung, ist aber für die Suche mithilfe API nicht auffindbar.
7. **Kein Wert**. Diese Bedingung trifft nicht zu. Bei Bedarf können Sie weitere Eigenschaften der Regel in anderen Abschnitten anpassen.
8. Erzwingen Sie bei Bedarf die Regel, indem Sie auf die Schaltfläche **Erzwingen** im unteren Bereich des Fensters klicken.

   Der Assistent zur Regelausführung wird gestartet. Folgen Sie den Anweisungen des Assistenten. Nach Abschluss des Assistenten wird die Regel ausgeführt und die Struktur der Untergruppen in der Untergruppe **Verwaltete Geräte\Cloud** entspricht der Struktur Ihrer Cloud-Segmente.
9. Klicken Sie auf die Schaltfläche **OK**.

Die Eigenschaften wurden eingerichtet und gespeichert.

Um die Regel Synchronisierung mit Cloud zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Konsolenbaum mit der rechten Maustaste auf den Namen des Knotens **Gerätesuche**.
2. Wählen Sie im Kontextmenü den Punkt **Eigenschaften** aus.
3. Wählen Sie im angezeigten Fenster **Eigenschaften** im Bereich **Abschnitte** den Punkt **Geräte verschieben** aus.
4. Deaktivieren Sie in der Liste der Regeln in dem Arbeitsbereich die Regel **Synchronisierung mit Cloud** und klicken Sie auf **OK**.

Die Regel ist deaktiviert und wird nicht mehr angewendet.

Bereitstellung von Kaspersky Security Center in Yandex.Cloud

Sie können Kaspersky Security Center in Yandex.Cloud bereitstellen. Es steht nur der Pay-per-use-Modus zur Verfügung - Cloud-Datenbanken werden nicht unterstützt.

In Yandex.Cloud stehen die folgenden Methoden für die Bereitstellung von Sicherheitsanwendungen zur Verfügung:

- Bereitstellung durch Bordmittel von Kaspersky Security Center mittels der Aufgabe zur *Remote-Installation* (Die Bereitstellung von Sicherheitsanwendungen ist nur dann möglich, wenn der Administrationsserver und die virtuellen Maschinen in dem gleichen Netzwerksegment geschützt werden)
- Bereitstellung mittels Bereitstellungsskripten

Für die Bereitstellung von Kaspersky Security Center in Yandex.Cloud benötigen Sie ein Service-Benutzerkonto für Yandex.Cloud. Sie müssen diesem Benutzerkonto die Berechtigung "marketplace.meteringAgent" geben und das Konto den virtuellen Maschinen zuordnen (Weitere Informationen entnehmen Sie bitte https://cloud.yandex.com/en).

Appendix

Diesem Abschnitt enthält Hilfe- und die Zusatzinformationen zur Nutzung von Kaspersky Security Center.

Zusatzoptionen

In diesem Abschnitt werden zusätzliche Funktionen von Kaspersky Security Center besprochen, welche die Möglichkeiten einer zentralisierten Programmverwaltung auf Client-Geräten erweitern.

Automatisierung der Programmfunktion von Kaspersky Security Center. Tool klakaut

Sie können Kaspersky Security Center mithilfe des Tools klakaut automatisieren. Das Tool klakaut und das entsprechende Hilfesystem befinden sich im Installationsordner von Kaspersky Security Center.

Arbeiten mit externen Instrumenten

Mithilfe von Kaspersky Security Center lässt sich eine Liste von *externen Werkzeugen* (im Weiteren auch *Tools*) erstellen. Das sind Programme, die für das Client-Gerät aus der Verwaltungskonsole mithilfe der Kontextmenü-Gruppe **Externe Tools** aufgerufen werden. Zu jedem Element der Tool-Liste wird ein separater Menüeintrag angelegt, mit dem die Verwaltungskonsole das dem Tool entsprechende Programm startet.

Das Programm wird im Administrator-Arbeitsplatz gestartet. Es kann als Argumente der Befehlszeile Attribute des Remote-Client-Geräts (NetBIOS-Name, DNS-Name, IP-Adresse) entgegennehmen. Die Verbindung zum Remote-Gerät kann über eine getunnelte Verbindung erfolgen.

Standardmäßig sind für jedes Client-Gerät auf der Liste mit externen Tools die folgenden Dienstprogramme verfügbar:

- **Remote-Diagnose** – Ferndiagnosetool von Kaspersky Security Center.
- **Remote-Desktop** ist eine Standard-Komponente von Microsoft Windows namens "Remotedesktopverbindung".
- **Computerverwaltung** – Standardkomponente von Microsoft Windows.

Um externe Tools hinzuzufügen oder zu löschen sowie ihre Einstellungen anzupassen,

Wählen Sie im Kontextmenü des Client-Gerätes den Punkt **Externe Tools → Benutzerdefinierte Tools konfigurieren** aus.

Das Fenster **Externe Tools** wird geöffnet. In diesem Fenster können Sie benutzerdefinierte Werkzeuge hinzufügen oder deren Einstellungen bearbeiten, indem Sie die Schaltflächen **Hinzufügen** und **Ändern** verwenden. Um ein benutzerdefiniertes Werkzeug zu entfernen, klicken Sie auf die Entfernen-Schaltfläche mit dem roten Kreuzsymbol ( ).

Modus des Administrationsagenten zum Klonen von Laufwerken

Das Klonen der Festplatte eines Referenzgerätes ist eine verbreitete Methode zur Installation von Software auf neuen Geräten. Wenn der Administrationsagent auf der Festplatte des Referenzgerätes während des Klonens im Standardmodus ausgeführt wird, kann das folgende Problem auftreten:

Nach der Bereitstellung des Referenz-Image der Festplatte mit dem Administrationsagenten auf den neuen Geräten werden diese Geräte in der Verwaltungskonsole mit dem gleichen Symbol dargestellt. Das Problem tritt auf, weil beim Klonen auf den neuen Geräten identische interne Daten gespeichert werden, die es dem Administrationsserver erlauben, das Gerät mit dem Symbol in der Verwaltungskonsole zu verknüpfen.

Die Probleme mit der inkorrekten Anzeige neuer Geräte in der Verwaltungskonsole nach dem Klonen können mithilfe des speziellen *Laufwerk klonen-Modus des Administrationsagenten* vermieden werden. Verwenden Sie diesen Modus, wenn Sie die Software (mit dem Administrationsagenten) auf neuen Geräten mittels der Laufwerk klonen-Methode verteilen.

Im Laufwerk klonen-Modus wird der Administrationsagent ausgeführt, stellt aber keine Verbindung mit Administrationsserver her. Beim Ausschalten des Laufwerk klonen-Modus löscht der Administrationsagent die internen Daten, aufgrund deren der Administrationsserver mehrere Geräte mit einem Symbol in der Verwaltungskonsole verknüpft. Nach Abschluss des Klonens des Referenzgerät-Images werden neue Geräte in der Verwaltungskonsole korrekt (als einzelne Symbole) angezeigt.

Handlungsempfehlung für das Laufwerkklonen des Administrationsagenten

1. Der Administrator installiert den Administrationsagenten auf dem Client-Gerät.
2. Der Administrator überprüft die Verbindung des Administrationsagenten mit dem Administrationsserver mithilfe des Dienstprogramms klnagchk.
3. Der Administrator aktiviert den "Laufwerk klonen"-Modus des Administrationsagenten.
4. Der Administrator installiert Software und Patches auf dem Gerät und führt eine beliebige Anzahl von Geräteneustarts aus.
5. Der Administrator nimmt das Klonen des Referenzgerät-Laufwerks auf beliebig vielen Geräten vor.
6. Für jede geklonte Kopie müssen folgende Bedingungen erfüllt sein:
   a. Der Geräte wurde geändert
   b. Das Gerät wurde Neu starten
   c. Der "Laufwerk klonen"-Modus wurde deaktiviert

Den "Laufwerk klonen"-Modus mithilfe des Tools "klmover" aktivieren und deaktivieren

Um den "Laufwerk klonen"-Modus des Administrationsagenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Starten Sie das Tool klmover auf dem Gerät mit dem installierten Administrationsagenten, das geklont werden soll.

   Das klmover-Dienstprogramm befindet sich im Installationsordner des Administrationsagenten.

2. Um den Modus zum Klonen von Laufwerken zu aktivieren, geben Sie in der Windows-Kommandozeile den Befehl ein:

   ```
   klmover -cloningmode 1
   ```

   Der Administrationsagent schaltet in den Modus zum Klonen von Laufwerken.

3. Um den aktuellen Status des den Modus zum Klonen von Laufwerken abzurufen, geben Sie in der Kommandozeile den folgenden Befehl ein:

   ```
   klmover -cloningmode
   ```

   Im Fenster des Tools wird angezeigt, ob der "Laufwerk klonen"-Modus aktiviert oder deaktiviert ist.

4. Um den den Modus zum Klonen von Laufwerken zu deaktivieren, geben Sie in der Kommandozeile des Tools den folgenden Befehl ein:

   ```
   klmover -cloningmode 0
   ```

Vorbereiten eines Referenzgeräts mit installiertem Administrationsagenten, um ein Betriebssystemabbild zu erstellen

Möglicherweise möchten Sie ein Betriebssystemabbild eines Referenzgeräts mit installiertem Administrationsagenten erstellen und das Abbild dann auf den vernetzten Geräten bereitstellen. In diesem Fall erstellen Sie das Betriebssystemabbild eines Referenzgeräts, auf dem der Administrationsagent noch nicht gestartet wurde. Wenn Sie den Administrationsagenten auf einem Referenzgerät starten, bevor ein Betriebssystemabbild erstellt wird, ist es für den Administrationsserver problematisch, die Geräte zu identifizieren, die von einem Betriebssystemabbild des Referenzgeräts bereitgestellt werden.

Um das Referenzgerät auf das Erstellen eines Betriebssystemabbilds vorzubereiten:

1. Stellen Sie sicher, dass auf dem Referenzgerät das Windows-Betriebssystem installiert ist, und installieren Sie die andere Software, die Sie auf diesem Gerät benötigen.

2. Gehen Sie auf dem Referenzgerät zu den Einstellungen für die Windows-Netzwerkverbindungen und trennen Sie das Referenzgerät von dem Netzwerk, in dem Kaspersky Security Center installiert ist.

3. Starten Sie auf dem Referenzgerät die lokale Installation des Administrationsagenten mithilfe der Datei setup.exe.

   Der Installationsassistent für den Kaspersky Security Center Administrationsagenten wird gestartet. Folgen Sie den Anweisungen des Assistenten.

4. Geben Sie auf der Seite **Administrationsserver** des Assistenten die IP-Adresse des Administrationsservers an.

   Wenn Sie die genaue Adresse des Administrationsservers nicht kennen, geben Sie localhost ein. Sie können die IP-Adresse später ändern, indem Sie das Tool Imover mit dem Parameter `-address` verwenden.

5. Deaktivieren Sie auf der Seite **Programm starten** des Assistenten die Option **Programm im Installationsvorgang starten**.

6. Nachdem die Installation des Administrationsagenten abgeschlossen wurde, erstellen Sie zuerst ein Betriebssystemabbild, bevor Sie das Gerät neu starten.

   Wenn Sie das Gerät neu starten, müssen Sie alle Vorbereitungen eines Referenzgeräts für die Erstellung eines Betriebssystemabbilds wiederholen.

7. Starten Sie auf dem Referenzgerät das Tool sysprep in der Befehlszeile und führen Sie den folgenden Befehl aus: `sysprep.exe /generalize /oobe /shutdown`.

Das Referenzgerät ist zum Erstellen eines Betriebssystemabbilds bereit.

Einstellungen des Empfangs von Nachrichten von der Komponente "Überwachung der Dateiintegrität" anpassen

Verwaltete Programme wie Kaspersky Security für Windows Server oder Kaspersky Security for Virtualization Light Agent senden Benachrichtigungen von der Komponente "Überwachung der Dateiintegrität" an Kaspersky Security Center. Kaspersky Security Center ermöglicht außerdem eine Untersuchung der Unveränderlichkeit von kritisch wichtigen Systembereichen (beispielsweise Webserver, Geldautomaten) und eine operative Reaktion auf Verstöße gegen die Integrität dieser Systeme. Zu diesem Zweck versendet die Komponente "Überwachung der Dateiintegrität" Benachrichtigungen an Sie. Die Komponente "Überwachung der Dateiintegrität" ermöglicht nicht nur die Überwachung des Dateisystems des Geräts, sondern auch seiner Registry-Hives, des Zustands seiner Firewall und des Zustands der angeschlossenen Hardware.

Kaspersky Security Center muss konfiguriert werden, um Benachrichtigungen der Komponente "Überwachung der Dateiintegrität" erhalten zu können, ohne Kaspersky Security für Windows Server oder Kaspersky Security for Virtualization Light Agent zu verwenden.

Um den Empfang von Benachrichtigungen von der Komponente "Überwachung der Dateiintegrität" anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsserver installiert ist, z. B. lokal mit dem Befehl "regedit" im Menü **Start** > **Ausführen**.

2. Rufen Sie den folgenden Abschnitt auf:

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - Für 64-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Erstellen Sie folgende Schlüssel:

   - Erstellen Sie den Schlüssel KLSRV_EVP_FIM_PERIOD_SEC, um den Zeitraum für die Zählung der Anzahl der verarbeiteten Ereignisse anzugeben. Geben Sie die folgenden Einstellungen an:

     a. Geben Sie als Schlüsselname KLSRV_EVP_FIM_PERIOD_SEC an.

     b. Geben Sie als Schlüsseltyp "DWORD" an.

     c. Legen Sie für den Zeitraum einen Wertebereich von 43.200 bis 172.800 Sekunden fest. Der Standardwert beträgt 86.400 Sekunden.

   - Erstellen Sie den Schlüssel KLSRV_EVP_FIM_LIMIT für die Beschränkung der Anzahl der übernommenen Ereignisse im angegebenen Zeitraum. Geben Sie die folgenden Einstellungen an:

     a. Geben Sie als Schlüsselname KLSRV_EVP_FIM_LIMIT an.

     b. Geben Sie als Schlüsseltyp "DWORD" an.

     c. Legen Sie für empfangene Ereignisse einen Wertebereich von 2.000 bis 50.000 fest. Standardmäßig beträgt die Anzahl der Ereignisse 20.000.

- Erstellen Sie den Schlüssel KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC für die Zählung der Ereignisse mit der Genauigkeit bis zum festgelegten Zeitraum. Geben Sie die folgenden Einstellungen an:

  a. Geben Sie als Schlüsselname KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC an.

  b. Geben Sie als Schlüsseltyp "DWORD" an.

  c. Legen Sie den Wertebereich von 120 bis 600 Sekunden fest. Standardmäßig beträgt das Zeitintervall 300 Sekunden.

- Erstellen Sie den Schlüssel KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC, damit das Programm nach dem angegebenen Zeitraum überprüft, ob die Anzahl der Ereignisse, die im Zeitraum verarbeitet wurden unter der festgelegten Beschränkung liegt. Die Untersuchung wird beim Erreichen der Beschränkung für die Aufnahme von Ereignisse ausgeführt. Wenn die Bedingung erfüllt ist, erfolgt eine erneute Speicherung der Ereignisse in der Datenbank. Geben Sie die folgenden Einstellungen an:

  a. Geben Sie als Schlüsselname KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC an.

  b. Geben Sie als Schlüsseltyp "DWORD" an.

  c. Legen Sie den Wertebereich von 600 bis 3.600 Sekunden fest. Standardmäßig beträgt das Zeitintervall 1.800 Sekunden.

Wenn keine Schlüssel erstellt werden, werden die Standardwerte verwendet.

4. Starten Sie den Dienst des Administrationsservers neu.

Die Beschränkungen des Empfangs von Ereignissen der Komponente "Überwachung der Dateiintegrität" sind nun konfiguriert. Die Ausführungsergebnisse der Komponente "Überwachung der Dateiintegrität" können Sie in den Berichten **Die 10 Regeln zur Überwachung der Dateiintegrität bzw. zur Überwachung der Systemintegrität, die auf den Geräten am häufigsten ausgelöst wurden** und **Die 10 Geräte, auf denen die Regeln zur Überwachung der Dateiintegrität bzw. zur Überwachung der Systemintegrität am häufigsten ausgelöst wurden** einsehen.

Wartung des Administrationsservers

Die Wartung des Administrationsservers ermöglicht die Freigabe von Speicherplatz im Ordner des Administrationsservers und das Reduzieren der Datenbankgröße, indem nicht mehr benötigte Objekte gelöscht werden. Dies trägt zu einer verbesserten Leistung und erhöhten Ausführungszuverlässigkeit der Anwendung bei. Es wird empfohlen, den Administrationsserver mindestens einmal wöchentlich zu warten.

Die Wartung des Administrationsservers erfolgt mithilfe der entsprechenden Aufgaben. Bei der Wartung des Administrationsservers führt das Programm die folgenden Aktionen aus:

- Es werden nicht benötigte Ordner und Dateien aus dem Ablageordner gelöscht.
- Es werden nicht benötigte Datensätze aus Tabellen gelöscht (auch als "hängender Zeiger" bekannt).
- Es wird der Cache geleert.
- Es wird die Datenbank gewartet (bei Verwendung von SQL Server oder PostgreSQL als DBMS):
  - Die Datenbank wird auf Fehler geprüft (nur SQL Server).
  - Die Datenbanken wird neu indiziert.

- Die Datenbankstatistik wird aktualisiert.
- Datenbank komprimieren (falls erforderlich).

So erstellen Sie die Aufgabe Wartung des Administrationsservers:

1. Wählen Sie in der Konsolenstruktur den Knoten des Administrationsservers, für den die Aufgabe *Wartung des Administrationsservers* erstellt werden soll.
2. Wählen Sie den Ordner **Aufgaben** aus.
3. Klicken Sie im Arbeitsbereich des Ordners **Aufgaben** auf die Schaltfläche **Neue Aufgabe**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
4. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten den Aufgabentyp **Wartung des Administrationsservers** und klicken Sie anschließend auf **Weiter**.
5. Wenn die Datenbank des Administrationsservers während der Wartung komprimiert werden muss, aktivieren Sie im Fenster **Einstellungen** des Assistenten das Kontrollkästchen **Datenbank komprimieren**.
6. Folgen Sie den weiteren Schritten des Assistenten.

Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsbereich des Ordners **Aufgaben** angezeigt. Für einen Administrationsserver kann nur eine Aufgabe des Typs *Wartung des Administrationsservers* ausgeführt werden. Wenn für den Administrationsserver bereits eine Aufgabe des Typs *Wartung des Administrationsservers* erstellt wurde, ist es nicht möglich, eine weitere Aufgabe des Typs *Wartung des Administrationsservers* zu erstellen.

Zugriff auf öffentliche DNS-Server

Wenn der Zugriff auf Kaspersky-Server über System-DNS nicht möglich ist, kann Kaspersky Security Center die folgenden öffentlichen DNS-Server in der angegebenen Reihenfolge verwenden:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Anfragen an diese DNS-Server können Domänenadressen und die öffentliche IP-Adresse des Administrationsservers enthalten, da das Programm eine TCP/UDP-Verbindung zum DNS-Server herstellt. Wenn Kaspersky Security Center einen öffentlichen DNS-Server verwendet, unterliegt die Datenverarbeitung der Datenschutzrichtlinie des entsprechenden Dienstes.

So konfigurieren Sie die Verwendung von öffentlichem DNS mithilfe des Tools "klscflag":

1. Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

2. Um die Verwendung von öffentlichen DNS zu deaktivieren, führen Sie den folgenden Befehl aus:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Um die Verwendung von öffentlichen DNS zu aktivieren, führen Sie den folgenden Befehl aus:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Fenster "Benachrichtigungsmethode"

Im Fenster **Benachrichtigungsmethode** können Sie die Benachrichtigungseinstellungen anpassen, um den Benutzer über die Installation des Zertifikats auf dem mobilen Gerät zu benachrichtigen.

- **QR-Code im Assistenten anzeigen**. Bei der Auswahl dieser Variante wird im letzten Schritt des Assistenten für die Verbindung eines mobilen Gerätes der Link zum Installationspaket angezeigt.

- **QR-Code an Benutzer senden**. Bei der Auswahl dieser Variante können Sie die Einstellungen für die Benachrichtigung des Benutzers über die Verbindung eines mobilen Geräts anpassen.

Im Einstellungsblock **Per E-Mail** können Sie die Benachrichtigungseinstellungen anpassen, um den Benutzer per E-Mail-Nachricht über die Installation des Zertifikates auf seinem mobilen Gerät zu benachrichtigen. Diese Benachrichtigungsmethode ist nur verfügbar wenn der SMTP-Server angepasst wurde.

Im Einstellungsblock **Mit SMS** können Sie die Benachrichtigungseinstellungen anpassen, um den Benutzer per SMS-Nachricht über die Installation des Zertifikates auf seinem mobilen Gerät zu benachrichtigen. Diese Benachrichtigungsmethode ist nur verfügbar wenn die SMS-Nachrichten angepasst wurden.

Über den Link **Nachricht bearbeiten** in den Einstellungsblöcken **Per E-Mail** und **Mit SMS** können Sie den Text der Benachrichtigung anzeigen und erforderlichenfalls bearbeiten.

Fenster Geräteauswahl

Wählen Sie in der Liste **Geräteauswahl** eine Auswahl. Die Liste enthält sowohl vordefinierte Auswahlen aus auch Auswahlen, die vom Benutzer erstellt wurden.

Details zu den Geräteauswahlen können Sie im Arbeitsbereich des Abschnitts **Geräteauswahlen** anzeigen.

Fenster "Name des zu erstellenden Objekts festlegen"

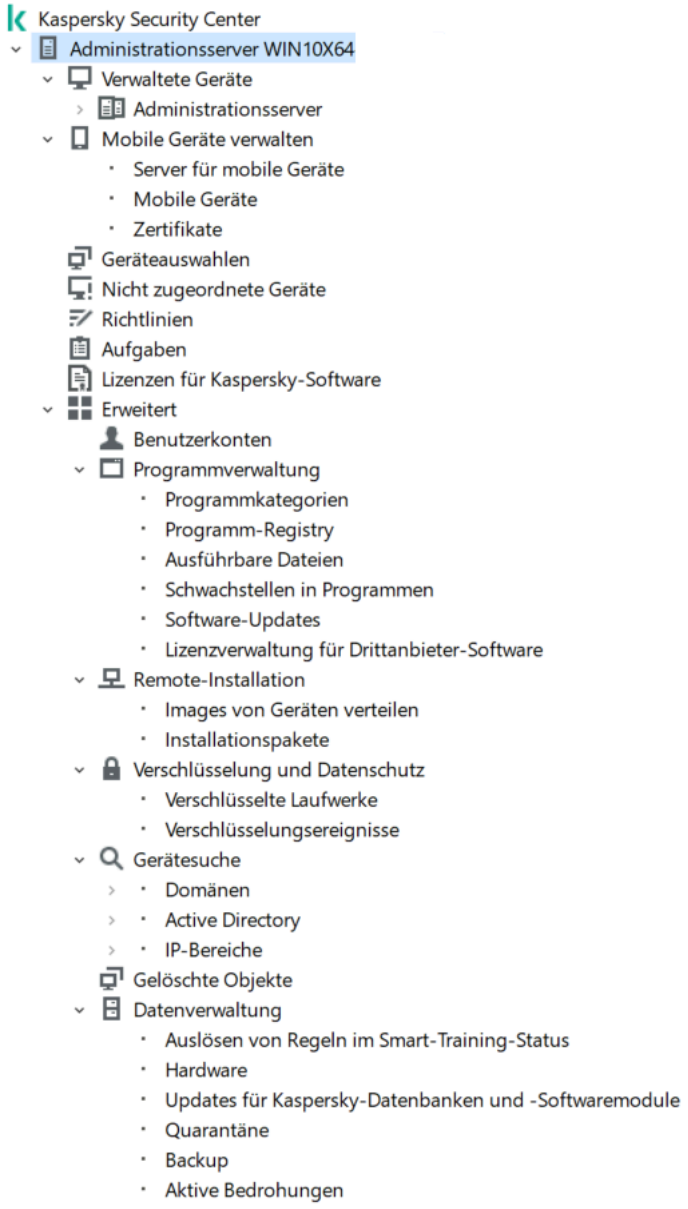
Geben Sie im Fenster den Namen des zu erstellenden Objekts an. Der Name darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

Besonderheiten der Verwaltungsoberfläche

Der Abschnitt beschreibt, wie das Programm Kaspersky Security Center von seinem Hauptfenster aus bedient wird.

Konsolenstruktur

Die Konsolenstruktur (s. Abb. unten) dient zur Anzeige der im Netzwerk angelegten Hierarchie der Administrationsserver, der Struktur ihrer Administrationsgruppen sowie anderer Objekte des Programms (z. B. Ordner **Datenverwaltung** und **Programmverwaltung**). Die Namensumgebung von Kaspersky Security Center kann mehrere Knoten mit Namen von Servern enthalten, welche die Netzwerkstruktur der Administrationsserver widerspiegeln.



Konsolenstruktur

Knoten "Administrationsserver"

Der Knoten **Administrationsserver –<Gerätename>** ist ein Container, der die Struktur des angegebenen Administrationsservers darstellt.

Der Arbeitsbereich des Knotens **Administrationsserver** enthält eine Übersicht über den aktuellen Status des Programms und der Geräte, die sich unter der Verwaltung des Administrationsservers befinden. Die Informationen im Arbeitsbereich sind auf Registerkarten verteilt:

- **Monitoring**. Zeigt Informationen über die Ausführung des Programms und den aktuellen Status der Client-Geräte in Echtzeit an. Wichtige Nachrichten für den Administrator (beispielsweise Nachrichten über Schwachstellen, Fehler, erkannte Viren) werden farbig hervorgehoben. Mithilfe der Links auf der Registerkarte **Monitoring** können Sie typische Administratoraufgaben ausführen (z. B. eine Sicherheitsanwendung auf Client-Geräten installieren und konfigurieren) und zu anderen Ordnern der Konsolenstruktur wechseln.

- **Statistik**. Enthält eine Auswahl von Diagrammen, die nach Themen (Schutzstatus, Antiviren-Statistik, Updates und andere) gruppiert sind. In den Diagrammen werden aktuelle Informationen über die Ausführung des Programms und den Zustand der Client-Geräte in grafischer Form dargestellt.

- **Berichte**. Enthält Vorlagen für die Berichte, die vom Programm erstellt werden. Auf dieser Registerkarte können Sie Berichte aus den vordefinierten Vorlagen erstellen sowie eigene Berichtsvorlagen erstellen.

- Fenster **Ereignisse**. Enthält Einträge über Ereignisse, die während der Ausführung des Programms registriert wurden. Zur besseren Lesbarkeit und Sortierung, werden die Einträge thematisch unterteilt. Auf dieser Registerkarte können Sie eine automatisch erstelle Ereignisauswahl anzeigen sowie Ihre eigenen Auswahlen erstellen.

Ordner im Knoten Administrationsserver

Der Knoten **Administrationsserver –<Gerätename>** enthält die folgenden Ordner:

- **Verwaltete Geräte**. Der Ordner Verwaltete Geräte dient zum Speichern, Darstellen, Konfigurieren und Ändern der Struktur von Administrationsgruppen, von Gruppenrichtlinien und von Gruppenaufgaben.

- **Verwaltung mobiler Geräte**. Dieser Ordner dient zur Verwaltung der mobilen Geräte. Der Ordner **Verwaltung mobiler Geräte** enthält folgenden Unterordner:

  - **Server für mobile Geräte**. Dient zur Verwaltung von iOS MDM-Servern.

  - **Mobile Geräte**. Dient zur Verwaltung von mobilen Geräten, KES und iOS MDM.

  - **Zertifikate**. Dient zur Verwaltung von Zertifikaten für mobile Geräte.

- **Geräteauswahlen**. Der Ordner dient zur schnellen Auswahl von Geräten, die bestimmten Kriterien entsprechen (Geräteauswahlen), aus der Gesamtheit der verwalteten Geräte. Beispielsweise können Sie schnell Geräte auswählen, auf denen keine Sicherheitsanwendung installiert ist, und zu diesen Geräten wechseln (deren Liste anzeigen). Mit den ausgewählten Geräten können Aktionen ausgeführt werden, beispielsweise können ihnen Aufgaben zugewiesen werden. Sie können vordefinierte Auswahlen verwenden oder Ihre eigenen (benutzerdefinierten) Auswahlen erstellen.

- **Nicht zugeordnete Geräte**. Dieser Ordner enthält eine Liste der Geräte, die keiner Administrationsgruppe angehören. Sie können mit den nicht zugeordneten Geräten Aktionen ausführen und sie z. B. in Administrationsgruppen verschieben oder Programme darauf installieren.

- **Richtlinien**. Dieser Ordner ist zur Anzeige und Erstellung von Richtlinien vorgesehen.

- **Aufgaben**. Dieser Ordner ist zur Anzeige und Erstellung von Aufgaben vorgesehen.
- **Lizenzen für Kaspersky-Software**. Enthält eine Liste der verfügbaren Lizenzschlüssel für die Kaspersky-Anwendungen. Im Arbeitsbereich des Ordners können Sie neue Lizenzschlüssel in den Schlüsselspeicher hinzufügen, Lizenzschlüssel auf die verwalteten Geräte verteilen oder einen Bericht über die Lizenzschlüsselnutzung anzeigen.
- **Erweitert**. Dieser Ordner enthält eine Reihe von Unterordnern, die den verschiedenen Funktionsgruppen des Programms entsprechen.

Ordner Erweitert. Ordner in der Konsolenstruktur verschieben

Zum Ordner **Erweitert** gehören folgende Unterordner:

- **Benutzerkonten**. Dieser Ordner enthält eine Liste der Benutzerkonten des Netzwerks.
- **Programmverwaltung**. Dieser Ordner dient der Verwaltung der auf den Netzwerkgeräten installierten Programme. Der Ordner **Programmverwaltung** enthält folgende Unterordner:
  - **Programmkategorien**. Der Ordner dient dazu, mit Programmkategorien zu arbeiten.
  - **Programm-Registry**. Enthält eine Liste von Programmen auf den Geräten mit installiertem Administrationsagenten.
  - **Ausführbare Dateien**. Enthält eine Liste ausführbarer Dateien, die sich auf den Client-Geräten mit installiertem Administrationsagenten befinden.
  - **Schwachstellen in Programmen**. Enthält eine Liste mit Schwachstellen in Programmen auf den Geräten mit installiertem Administrationsagenten.
  - **Programm-Updates**. Enthält eine Liste der vom Administrationsserver empfangenen Programm-Updates, die auf die Geräte verteilt werden können.
  - **Verwendung von Drittanbieter-Lizenzen**. Enthält eine Liste der lizenzierten Programmgruppen. Mithilfe von lizenzierten Programmgruppen kann die Nutzung von Lizenzen für Drittanbieter-Programme (d. h. keine Kaspersky-Anwendungen) und die Verletzung der Lizenzbeschränkungen überwacht werden.
- **Remote-Installation**. Dieser Ordner dient zur Verwaltung der Remote-Installationen von Betriebssystemen und Programmen. Der Ordner **Remote-Installation** enthält folgende Unterordner:
  - **Geräten-Images verteilen**. Der Ordner dient der Bereitstellung von Betriebssystem-Images auf die Geräte.
  - **Installationspakete**. Dieser Ordner enthält eine Liste der Installationspakete, die zur Remote-Installation von Programmen auf den Client-Geräten verwendet werden können.
- **Verschlüsselung und Datenschutz**. Dieser Ordner wird zur Verwaltung der Datenverschlüsselung auf Festplatten und Wechseldatenträgern verwendet.
- **Netzwerkabfrage**. Dieser Ordner zeigt das Netzwerk an, in dem der Administrationsserver installiert ist. Der Administrationsserver erhält Informationen über die Struktur des Netzwerks und der darin befindlichen Geräte durch regelmäßige Abfragen des Windows-Netzwerks, der IP-Subnetze und der Active Directory® im Unternehmensnetzwerk. Die Suchergebnisse werden in den Arbeitsplätzen der entsprechenden Ordner **Domänen**, **IP-Bereiche** und **Active Directory** angezeigt.

- **Datenverwaltung**. Dieser Ordner dient der Arbeit mit Objekten, die zur Überwachung des Status der Geräte und für deren Bearbeitung verwendet werden. Der Ordner **Datenverwaltung** enthält folgende Unterordner:
  - **Adaptive Erkennung von Anomalien**. Enthält eine Liste an Funden, welche durch die Regeln von Kaspersky Endpoint Security im Smart Training-Modus auf Client-Geräten erkannt wurden.
  - **Updates und Patches für Software von Kaspersky**. Enthält eine Liste der vom Administrationsserver empfangenen Updates, die auf die Geräte verteilt werden können.
  - **Hardware**. Der Ordner enthält eine Liste der im Unternehmensnetzwerk angeschlossenen Hardware.
  - **Quarantäne**. Der Ordner enthält eine Liste der Objekte, die von Antiviren-Programmen in die Quarantäne-Ordner auf den Geräten verschoben wurden.
  - **Backup**. Enthält eine Liste der Backup-Kopien von Dateien, die während der Desinfektion auf den Geräten gelöscht oder verändert wurden.
  - **Unverarbeitete Dateien**. Der Ordner enthält eine Liste der Dateien, für die von Antiviren-Programmen die Notwendigkeit einer verschobenen Desinfektion bestimmt wurde.

Sie können die Auswahl der Unterordner des Ordners **Erweitert** verändern. Unterordner, die aktiv verwendet werden, können aus dem Ordner **Erweitert** auf eine höhere Ebene verschoben werden. Ordner, die nur selten verwendet werden, können in den Ordner **Erweitert** verschoben werden.

*Gehen Sie folgendermaßen vor, um einen Unterordner aus dem Ordner **Erweitert** zu verschieben:*

1. Wählen Sie in der Konsolenstruktur den Unterordner aus, den Sie aus dem Ordner **Erweitert** verschieben möchten.
2. Wählen Sie im Kontextmenü des Unterordners den Punkt **Ansicht → Verschieben aus dem Ordner Erweitert**.

Sie können einen Unterordner im Arbeitsbereich des Ordners **Erweitert** im Block mit dem Namen des Unterordners aus dem Ordner **Erweitert** auch mithilfe des Links **Verschieben aus dem Ordner Erweitert** verschieben.

*Gehen Sie folgendermaßen vor, um einen Unterordner in den Ordner **Erweitert** zu verschieben:*

1. Wählen Sie in der Konsolenstruktur den Unterordner aus, der in den Ordner **Erweitert** verschoben werden soll.
2. Wählen Sie im Kontextmenü des Unterordners den Punkt **Ansicht → In den Ordner Erweitert verschieben**.

Wie Daten im Arbeitsbereich aktualisiert werden

Bei Kaspersky Security Center werden Daten im Arbeitsbereich (z.B. Gerätestatus, Statistik, Berichte) automatisch nicht aktualisiert.

Um Daten im Arbeitsbereich zu aktualisieren, führen Sie eine der folgenden Aktionen aus:

- Drücken Sie die Taste **F5**.
- Klicken Sie mit der rechten Maustaste auf das Objekt in der Konsolenstruktur und wählen Sie **Aktualisieren** aus.
- Klicken Sie im Arbeitsbereich auf das Aktualisieren-Symbol ().

Wie in der Konsolenstruktur navigiert wird

Um in der Konsolenstruktur zu navigieren, können Sie in der Symbolleiste auf folgende Schaltflächen klicken:

-  – Für einen Schritt zurück
-  – Für einen Schritt nach vorn
-  – Um die nächsthöhere Ebene zu wechseln

Außerdem können Sie die Navigationskette in der rechten oberen Ecke des Arbeitsbereiches verwenden. Die Navigationskette enthält den kompletten Pfad zum Ordner der Konsolenstruktur, in dem Sie sich gegenwärtig befinden. Mit Ausnahme des letzten Elements fungieren alle Elemente der Kette als Links auf die Objekte der Konsolenstruktur.

Wie das Eigenschaftenfenster eines Objekts im Arbeitsbereich geöffnet wird

Die Eigenschaften der meisten Objekte der Verwaltungskonsole lassen sich im Eigenschaftenfenster ändern.

Gehen Sie wie folgt vor, um das Eigenschaftenfenster eines Objekts im Arbeitsbereich zu öffnen:

- Öffnen Sie das Kontextmenü des Objekts, und wählen Sie **Eigenschaften** aus.
- Wählen Sie das Objekt aus, und drücken Sie die Tastenkombination **ALT+ENTER**.

Wie eine Gruppe von Objekten im Arbeitsbereich ausgewählt wird

Sie können eine Gruppe von Objekten im Arbeitsbereich auswählen. Mit einer Gruppe von Objekten können Sie beispielsweise bestimmte Geräte auswählen und Aufgaben für sie anlegen.

Gehen Sie wie folgt vor, um einen Objektbereich auszuwählen:

1. Wählen Sie das erste Objekt des Bereichs aus, und drücken Sie die Taste **Umschalt**.
2. Halten Sie die **Umschalt**-Taste gedrückt, und wählen Sie das letzte Objekt des Bereichs aus.

   Dadurch wird der Bereich ausgewählt.

Um individuelle Objekte in einer Gruppe zusammenzufassen, gehen Sie wie folgt vor:

1. Wählen Sie das erste Objekt in der Gruppe aus, und drücken Sie die Taste **Strg**.
2. Halten Sie die Taste **Strg** gedrückt und wählen Sie die übrigen Objekte der Gruppe.

Dadurch werden die Objekte in einer Gruppe zusammengefasst.

Wie die Auswahl von Spalten im Arbeitsbereich geändert wird

In der Verwaltungskonsole können Sie die Auswahl an Spalten ändern, die im Arbeitsbereich angezeigt werden.

Um die Auswahl an Spalten im Arbeitsbereich zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur das Objekt aus, für das Sie die Spalten ändern wollen.
2. Öffnen Sie im Arbeitsbereich des Ordners über den Link **Spalten hinzufügen oder löschen** das Einstellungsfenster für die Auswahl von Spalten.
3. Erstellen Sie im Fenster **Spalten hinzufügen oder löschen** eine Auswahl von Spalten für die Anzeige.

Hilfe

In diesem Abschnitt finden Sie eine tabellarische Übersicht zum Kontextmenü der Objekte der Verwaltungskonsole und zum Status der Objekte im Konsolenbaum und im Arbeitsbereich.

Befehle des Kontextmenüs

Dieser Abschnitt enthält ein Objektverzeichnis der Verwaltungskonsole und eine entsprechende Punkteauswahl des Kontextmenüs (siehe Tabelle unten).

Elemente des Kontextmenüs der Objekte in der Verwaltungskonsole

Objekt	Menüpunkt	Zweck des Menüpunkts
Allgemeine Einträge im Kontextmenü	**Suchen**	Fenster Suche nach Geräten öffnen
	Aktualisieren	Anzeige des ausgewählten Objekts aktualisieren.
	Liste exportieren	Aktuelle Liste in Datei exportieren
	Eigenschaften	Eigenschaftenfenster des ausgewählten Objekts öffnen
	Ansicht → Spalten hinzufügen oder löschen	Spalten in der Objekttabelle im Arbeitsbereich hinzufügen oder löschen.
	Ansicht → Große Symbole	Objekte im Arbeitsbereich als große Symbole anzeigen lassen.
	Ansicht → Kleine Symbole	Objekte im Arbeitsbereich als kleine Symbole anzeigen lassen.
	Ansicht → Liste	Objekte im Arbeitsbereich in Form einer Liste anzeigen.
	Ansicht → Tabelle	Objekte im Arbeitsbereich in Form einer Tabelle anzeigen.
	Ansicht → Einstellungen	Anzeige der Elemente der Verwaltungskonsole anpassen.
Kaspersky Security Center	**Neu → Administrationsserver**	Administrationsserver in Konsolenstruktur einfügen
<Name des Administrationsservers>	**Mit dem Administrationsserver verbinden**	Stellt eine Verbindung zum Administrationsserver her.
	Vom Administrationsserver trennen	Trennt die Verbindung zum Administrationsserver.
Verwaltete Geräte	**Programm installieren**	Startet den Assistenten für Remote-Installationen einer Anwendung.
	Ansicht → Benutzeroberfläche anpassen	Anzeige für die Elemente der Benutzeroberfläche anpassen.
	Entfernen	Administrationsserver aus Konsolenstruktur entfernen
	Programm installieren	Startet den Assistenten für Remote-Installationen für die Administrationsgruppe.
	Virenzähler zurücksetzen	Virenzähler für die Geräte der Administrationsgruppe zurücksetzen.
	Bericht über Bedrohungen anzeigen	Bericht über Bedrohungen und Virenaktivität der Geräte anlegen, die zu einer Administrationsgruppe gehören.
	Neu → Gruppe	Administrationsgruppe anlegen
	Alle Aufgaben → Neue Gruppenstruktur	Struktur der Administrationsgruppen anhand der Domänenstruktur oder der Struktur des Active Directory anlegen
	Alle Aufgaben → Nachricht anzeigen	Startet den Assistenten für das Erstellen einer Nachricht an Benutzer für die Geräte der Administrationsgruppe.
Verwaltete Geräte → Administrationsserver	**Neu → Sekundärer Administrationsserver**	Startet den Assistenten für das Hinzufügen eines sekundären Administrationsservers.
	Neu → Virtueller Administrationsserver	Startet den Assistenten für das Erstellen eines virtuellen Administrationsservers.
Verwaltung mobiler Geräte → Mobile Geräte	**Neu → Mobiles Gerät**	Verbindet ein neues mobiles Gerät des Benutzers.

Objekt	Menüpunkt	Zweck des Menüpunkts
Verwaltung mobiler Geräte → Zertifikate	**Neu → Zertifikat**	Erstellt ein Zertifikat.
	Erstellen → Mobiles Gerät	Verbindet ein neues mobiles Gerät des Benutzers.
Geräteauswahlen	**Neu → Neue Auswahl**	Geräteauswahl erstellen.
	Alle Aufgaben → Importieren	Auswahl aus Datei importieren.
Lizenzen für Kaspersky-Software	**Aktivierungscode oder Schlüsseldatei hinzufügen**	Fügt einen Lizenzschlüssel zu der Datenverwaltung des Administrationsservers hinzu.
	Programm aktivieren	Startet den Assistenten für das Erstellen einer Aufgabe zur Programmaktivierung.
	Bericht über die Lizenzschlüsselnutzung	Erstellt einen Bericht über die Lizenzschlüssel auf Client-Geräten und zeigt diesen Bericht an.
Programmverwaltung → Programmkategorien	**Neu → Kategorie**	Programmkategorie erstellen
Programmverwaltung → Programm-Registry	**Filter**	Filter für die Programmliste einstellen.
	Zu überwachende Programme	Veröffentlichung von Ereignissen, die mit Programminstallationen in Verbindung stehen.
	Nicht installierte Programme löschen	Informationen über Programme, die nicht mehr auf den Geräten des Netzwerks installiert sind, aus der Liste löschen.
Programmverwaltung → Software-Updates	**Lizenzverträge für Updates akzeptieren**	Lizenzverträge für Programm-Updates akzeptieren.
Programmverwaltung → Verwendung von Drittanbieter-Lizenzen	**Neu → Lizenzierte Programmgruppe**	Erstellt eine lizenzierte Programmgruppe.
Remote-Installation → Installationspakete	**Aktuelle Programmversionen anzeigen**	Liste der aktuellen Versionen von Kaspersky-Anwendungen ansehen, die auf Kaspersky-Internetservern zur Verfügung stehen.
	Neu → Installationspaket	Erstellt ein Installationspaket.
	Alle Aufgaben → Datenbanken aktualisieren	Programm-Datenbanken in den Installationspaketen aktualisieren.
	Alle Aufgaben → Gemeinsame Liste der autonomen Pakete anzeigen	Gemeinsame Liste der autonomen Installationspakete ansehen, die für Installationspakete erstellt wurden.
Gerätesuche → Domänen	**Alle Aufgaben → Geräteaktivität**	Einstellungen für die Reaktion des Administrationsservers auf fehlende Aktivität von Geräten im Netzwerk konfigurieren
Gerätesuche → IP-Bereiche	**Neu → IP-Bereich**	Erstellt einen IP-Bereich.
Datenverwaltung → Updates für Kaspersky-Datenbanken und -Softwaremodule	**Updates herunterladen**	Öffnet das Eigenschaftenfenster der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers.
	Einstellungen des Update-Downloads	Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers anpassen.
	Bericht über verwendete Antiviren-Datenbanken	Bericht über Datenbankversionen anlegen und anzeigen
	Alle Aufgaben → Update-Datenverwaltung leeren	Update-Datenverwaltung des Administrationsservers leeren
Datenverwaltung → Hardware	**Neu → Gerät**	Netzwerkgerät erstellen.

Liste der verwalteten Geräte. Beschreibung von Spalten

Die nachfolgende Tabelle enthält Namen und Beschreibungen der Spalten der Liste der verwalteten Geräte.

Spaltenwerte der Liste der verwalteten Geräte

Spaltenname	Wert
Name	NetBIOS-Name des Client-Geräts. Die Symbolbeschreibungen für die Gerätenamen finden Sie im Appendix.
Typ des Betriebssystems	Betriebssystem-Typ des Client-Geräts.
Windows-Domäne	Name der Windows-Domäne, zu welcher das Client-Gerät gehört.
Administrationsagent ist installiert	Ergebnis der Installation des Administrationsagenten auf dem Client-Gerät: *Ja*, *Nein*, *Unbekannt*.
Administrationsagent wird ausgeführt	Ergebnis der Funktion des Administrationsagenten: *Ja*, *Nein*, *Unbekannt*.
Echtzeitschutz	Die Sicherheitsanwendung wurde installiert: *Ja*, *Nein*, *Unbekannt*.
Letzte Verbindung mit dem Administrationsserver	Zeitraum seit der letzten Verbindung des Client-Geräts mit dem Administrationsserver.
Letzte Aktualisierung der Antiviren-Datenbanken	Der Zeitraum, der seit der letzten Aktualisierung der verwalteten Geräte vergangen ist.
Status	Aktueller Status des Client-Geräts: *OK*, *Kritisch*, *Warnung*.

Spaltenname	Wert
Statusbeschreibung	Bedingungen für den Wechsel des Status des Client-Geräts zu *Kritisch* oder *Warnung*. Der Gerätestatus wechselt unter folgenden Bedingungen zu *Warnung* oder *Kritisch*: • Es wurde keine Sicherheitsanwendung installiert. • Zu viele Viren gefunden. • Die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die der Administrator festgelegt hat. • Die letzte Schadsoftware-Untersuchung liegt lange zurück. • Die Datenbanken sind veraltet. • Die letzte Verbindung liegt lange zurück. • Aktive Bedrohungen werden erkannt. • Neustart erforderlich. Das Gerät kann aus einem der folgenden Gründe neu gestartet werden: • Aus unbekanntem Grund neu gestartet. • Programm wird erst nach Neustart ausgeführt. • Um das Update abzuschließen, ist ein Neustart erforderlich; das Programm ist jedoch funktionsfähig. • Zum Start des Updates ist ein Neustart erforderlich. • Zum Abschließen der Untersuchung oder Desinfektion ist ein Neustart erforderlich. • Um die Remote-Installation bzw. -Deinstallation abzuschließen, ist ein Neustart erforderlich. • Abschließen der Datenverschlüsselung auf der Festplatte. Bei der Konfiguration der Änderung des Gerätezustands können Sie Gründe angeben. • Es sind inkompatible Programme installiert. • Es wurden Schwachstellen in Programmen erkannt. • Die letzte Suche nach Windows-Updates liegt lange zurück. • Ungültiger Verschlüsselungsstatus. • Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie. • Es wurden unbearbeitete Sicherheitsprobleme erkannt • Gerätestatus wird vom Programm bestimmt. • Kein Platz auf dem Datenträger des Geräts. • Die Lizenz läuft bald ab. Der Gerätestatus wechselt aus folgenden Gründen nur zu *Kritisch*: • Lizenz abgelaufen. • Das Gerät wird nicht mehr verwaltet. • Der Schutz ist deaktiviert. • Die Sicherheitsanwendung wurde nicht gestartet. Die verwalteten Kaspersky-Anwendungen auf den Client-Geräten können die Liste der Statusbeschreibungen ergänzen. Kaspersky Security Center kann die Beschreibung des Status des Client-Geräts von den verwalteten Kaspersky-Anwendungen auf diesem Gerät erhalten. Wenn der Status, der dem Gerät durch die verwalteten Programme zugewiesen wurde, nicht mit dem von Kaspersky Security Center zugewiesenen Status übereinstimmt, wird in der Verwaltungskonsole der für die Sicherheit des Geräts kritischste Status angezeigt. Wenn z. B. eines der verwalteten Programme dem Gerät den Status *Kritisch*, Kaspersky Security Center jedoch den Status *Warnung* zugewiesen hat, wird in der Verwaltungskonsole für das Gerät der Status *Kritisch* sowie die Beschreibung dieses Status vom verwalteten Programm angezeigt.
Information aktualisiert	Zeitraum seit der letzten erfolgreichen Synchronisierung des Client-Gerätes mit dem Administrationsserver (d. h. seit der letzten Netzwerkabfrage).
DNS-Name	Name der DNS-Domäne des Client-Geräts.
DNS-Domäne	Primäres DNS-Suffix.
IP-Adresse	IP-Adresse des Client-Geräts. Es wird empfohlen, eine IPv4-Adresse zu verwenden.
Zuletzt im Netzwerk sichtbar	Dauer der Sichtbarkeit des Client-Geräts im Netzwerk.
Letzte vollständige Untersuchung	Datum und Uhrzeit der letzten Untersuchung des Client-Geräts, die auf Benutzeranfrage von einer Sicherheitsanwendung ausgeführt wurde.
Gesamtzahl der gefundenen Bedrohungen	Anzahl der gefundenen Bedrohungen.
Status des Echtzeitschutzes	Echtzeitschutz-Status: *Wird gestartet, Wird ausgeführt, Wird ausgeführt (maximaler Schutz), Wird ausgeführt (maximale Geschwindigkeit), Wird ausgeführt (empfohlene Einstellungen), Wird ausgeführt (benutzerdefinierte Einstellungen), Beendet, Angehalten, Fehlgeschlagen*.
IP-Adresse der Verbindung	IP-Adresse der Verbindung mit dem Kaspersky Security Center Administrationsserver.
Version des Administrationsagenten	Version des Administrationsagenten.
Programmversion	Version der Sicherheitsanwendung, die auf dem Client-Gerät installiert ist.

Spaltenname	Wert
Veröffentlichungsdatum der Antiviren-Datenbanken	Version der Antiviren-Datenbanken.
Letzter Systemstart	Datum und Uhrzeit des letzten Einschaltens des Client-Geräts.
Neustart erforderlich	Neustart des Client-Geräts ist erforderlich.
Verteilungspunkt	Name des Geräts, das die Rolle des Verteilungspunkts für dieses Client-Gerät übernimmt.
Beschreibung	Beschreibung des Client-Geräts, die beim Scannen des Netzwerks abgefragt wurde.
Verschlüsselungsstatus	Status der Datenverschlüsselung des Client-Geräts.
WUA-Status	Status des Windows Update-Agent des Client-Geräts. Der Wert *Ja* bezeichnet Client-Geräte, die Updates über Windows Update vom Administrationsserver empfangen. Der Wert *Nein* bezeichnet Client-Geräte, die Updates über Windows Update aus anderen Quellen empfangen.
Bitzahl des Betriebssystems	Bitanzahl des Betriebssystems des Client-Geräts.
Status des Schutzes vor Spam	Status der Komponente "Spam-Schutz": *Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehlgeschlagen, Unbekannt*
Status des Schutzes vor Datenverlust	Statuswerte der Komponente "Schutz vor Datenverlust": *Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehlgeschlagen, Unbekannt*
Status des Schutzes der Server für die Zusammenarbeit	Statuswerte der Komponente "Inhaltsfilterung": *Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehlgeschlagen, Unbekannt*
Status des Antiviren-Schutzes von Mail-Servern	Statuswerte der Komponente für den Antiviren-Schutz von Mail-Servern: *Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehlgeschlagen, Unbekannt*
Status der Komponente "Endpoint Sensor"	Statuswerte der Komponente "Endpoint Detection and Response" (KATA): *Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehlgeschlagen, Unbekannt*
Erstellt	Zeitpunkt, zu dem das Symbol für <Gerätename> erstellt wurde. Dieses Attribut wird verwendet, um verschiedene Ereignisse miteinander zu vergleichen.
Name des virtuellen oder sekundären Administrationsservers	Name des virtuellen oder sekundären Administrationsservers. Diese Spalte ist nur in Listen verfügbar, die Geräte von verschiedenen Administrationsservern enthalten.
Übergeordnete Gruppe	Name der Administrationsgruppe, in der sich das Symbol für <Gerätename> befindet. Diese Spalte ist nur in Listen verfügbar, die Geräte von verschiedenen Administrationsservern enthalten.
Verwaltung erfolgt durch anderen Administrationsserver	Der Parameter kann einen der folgenden Werte annehmen: • Richtig, wenn sich während der Remote-Installation von Sicherheitsanwendungen auf dem Gerät herausstellt, dass das Gerät von einem anderen Administrationsserver verwaltet wird. • Ansonsten: Falsch.
Build-Version des Betriebssystems	Versionsnummer des Betriebssystems. Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Suche nach allen Versionsnummern mit Ausnahme der angegebenen anpassen.
Release-ID des Betriebssystems	Release-Identifikator (ID) des Betriebssystems Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-ID haben muss. Sie können auch eine Suche nach allen Release-ID-Nummern anpassen und bestimmte Versionsnummern von der Suche ausschließen.

Statusmeldungen der Geräte, Aufgaben und Richtlinien

In der untenstehenden Tabelle befindet sich ein Verzeichnis von Zeichen, die in der Konsolenstruktur und im Arbeitsbereich der Verwaltungskonsole neben den Namen der Geräte, Aufgaben und Richtlinien erscheinen. Diese Zeichen erläutern den Status der Objekte.

Statusmeldungen der Geräte, Aufgaben und Richtlinien

Zeichen	Status
	Gerät mit Betriebssystem für Workstations, das im Netzwerk gefunden wurde und nicht zu einer Administrationsgruppe gehört
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und den Status *OK* aufweist.
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und den Status *Warnung* aufweist.
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und den Status *Kritisch* aufweist.
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und dessen Verbindung zum Administrationsserver unterbrochen wurde
	Gerät mit Betriebssystem für Server, das im Netzwerk gefunden wurde und nicht zu einer Administrationsgruppe gehört
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und den Status *OK* aufweist.
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und den Status *Warnung* aufweist.
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und den Status *Kritisch* aufweist.
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und dessen Verbindung zum Administrationsserver unterbrochen wurde
	Mobile Geräte, die im Netzwerk gefunden wurden und nicht zu einer Administrationsgruppe gehören.
	Mobile Geräte, die zu einer Administrationsgruppe gehören und den Status *OK* haben.
	Mobile Geräte, die zu einer Administrationsgruppe gehören und den Status *Warnung* haben.
	Mobile Geräte, die zu einer Administrationsgruppe gehören und den Status *Kritisch* haben.
	Mobile Geräte, die zu einer Administrationsgruppe gehören, deren Verbindung zum Administrationsserver unterbrochen ist.
	Gerät mit Schutz auf UEFI-Ebene, das im Netzwerk gefunden wurde und nicht zu einer Administrationsgruppe gehört. Gerät mit Schutz auf UEFI-Ebene im Netzwerk.
	Gerät mit Schutz auf UEFI-Ebene, das im Netzwerk gefunden wurde und nicht zu einer Administrationsgruppe gehört. Gerät mit Schutz auf UEFI-Ebene, das sich nicht im Netzwerk befindet.
	Gerät mit Schutz auf UEFI-Ebene, das zu einer Administrationsgruppe gehört und den Status *OK* aufweist. Gerät mit Schutz auf UEFI-Ebene im Netzwerk.
	Gerät mit Schutz auf UEFI-Ebene, das zu einer Administrationsgruppe gehört und den Status *OK* aufweist. Gerät mit Schutz auf UEFI-Ebene, das sich nicht im Netzwerk befindet.
	Gerät mit Schutz auf UEFI-Ebene, das zu einer Administrationsgruppe gehört und den Status *Warnung* aufweist. Gerät mit Schutz auf UEFI-Ebene im Netzwerk.
	Gerät mit Schutz auf UEFI-Ebene, das zu einer Administrationsgruppe gehört und den Status *Warnung* aufweist. Gerät mit Schutz auf UEFI-Ebene, das sich nicht im Netzwerk befindet.
	Gerät mit Schutz auf UEFI-Ebene, das zu einer Administrationsgruppe gehört und den Status *Kritisch* aufweist. Gerät mit Schutz auf UEFI-Ebene im Netzwerk.
	Gerät mit Schutz auf UEFI-Ebene, das zu einer Administrationsgruppe gehört und den Status *Kritisch* aufweist. Gerät mit Schutz auf UEFI-Ebene, das sich nicht im Netzwerk befindet.
	Aktive Richtlinie.

	Inaktive Richtlinie.
	Aktive Richtlinie, die von der auf dem primären Administrationsserver erstellten Gruppe vererbt wurde.
	Eine aktive Richtlinie, die von einer Gruppe einer übergeordneten Hierarchieebene vererbt wurde.
	Aufgabe (Gruppenaufgabe, Aufgabe des Administrationsservers oder für eine Reihe von Geräten) mit dem Zustand *Wartet auf Ausführung* oder *Erfolgreich beendet*.
	Aufgabe (Gruppenaufgabe, Aufgabe des Administrationsservers oder für eine Reihe von Geräten) mit dem Zustand *Wird ausgeführt*.
	Aufgabe (Gruppenaufgabe, Aufgabe des Administrationsservers oder für eine Reihe von Geräten) mit dem Zustand *Fehlgeschlagen*.
	Aufgabe, die von einer auf dem primären Administrationsserver erstellten Gruppe vererbt wurde.
	Eine Aufgabe, die von einer übergeordneten Hierarchieebene vererbt wurde.

Symbole der Status der Dateien in der Verwaltungskonsole

Für die Vereinfachung der Arbeit mit den Dateien in der Kaspersky Security Center Verwaltungskonsole werden neben den Namen der Dateien Symbole angezeigt (s. Tabelle unten). Die Symbole geben Auskunft über den Status, welcher der jeweiligen Datei von den verwalteten Kaspersky-Anwendungen auf den Client-Geräten zugewiesen wird. Die Symbole werden in den Arbeitsbereichen der Ordner **Quarantäne**, **Backup** und **Aktive Bedrohungen** angezeigt.

Seinen Status enthält ein Objekt von Kaspersky Endpoint Security, das auf dem Client-Gerät installiert ist, auf der sich das Objekt befindet.

Übereinstimmung der Symbole mit den Status der Dateien

Zeichen	Status
	Datei mit dem Status *Infiziert*.
	Datei mit dem Status *Warnung* oder *Möglicherweise infiziert*.
	Datei mit dem Status *Vom Benutzer hinzugefügt*.
	Datei mit dem Status *Fehlalarm*.
	Datei mit dem Status *Desinfiziert*.
	Datei mit dem Status *Gelöscht*.
	Datei im Ordner **Quarantäne** und mit dem Status *Virusfrei*, *Mit Kennwort geschützt* oder *Muss an Kaspersky gesendet werden*. Wenn neben dem Symbol keine Beschreibung des Status angezeigt wird, dann hat die verwaltete Kaspersky-Anwendung auf dem Client-Gerät einen unbekannten Status an Kaspersky Security Center übermittelt.
	Datei im Ordner **Backup** und mit dem Status *Virusfrei*, *Mit Kennwort geschützt* oder *Muss an Kaspersky gesendet werden*. Wenn neben dem Symbol keine Beschreibung des Status angezeigt wird, dann hat die verwaltete Kaspersky-Anwendung auf dem Client-Gerät einen unbekannten Status an Kaspersky Security Center übermittelt.
	Datei im Ordner **Aktive Bedrohungen** und mit dem Status *Virusfrei*, *Mit Kennwort geschützt* oder *Muss an Kaspersky gesendet werden*. Wenn neben dem Symbol keine Beschreibung des Status angezeigt wird, dann hat das verwaltete Kaspersky-Programm auf dem Client-Gerät einen unbekannten Status an Kaspersky Security Center übermittelt.

Suche und Export von Daten

Dieser Abschnitt enthält Informationen zu den Methoden der Suche und des Exports von Daten.

Suche nach Geräten

Kaspersky Security Center ermöglicht eine Suche der Geräte auf der Grundlage der angegebenen Kriterien. Suchergebnisse können in einer Textdatei gespeichert werden.

Mit der Suchfunktion können folgende Geräte gefunden werden:

- Client-Geräte der Administrationsgruppen des Administrationsservers und seiner sekundären Server.
- Nicht zugeordnete Geräte, die von einem Administrationsserver und dessen sekundären Servern verwaltet werden.

Um die Suche von Client-Geräten einer Administrationsgruppe auszuführen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner der Administrationsgruppe aus.
2. Klicken Sie mit der rechten Maustaste auf den Ordner der Administrationsgruppe und wählen Sie **Suchen** aus.
3. Geben Sie auf den Registerkarten des Fensters **Suchen** die Kriterien an, nach denen die Client-Geräte gesucht werden sollen, und klicken Sie auf die Schaltfläche **Suchen**.

   Daraufhin werden die Geräte, die den angegebenen Suchkriterien entsprechen, in der Tabelle im unteren Bereich des Fensters **Suchen** angezeigt.

Für die Suche von nicht zugeordneten Geräten gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Nicht zugeordnete Geräte** aus.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Nicht zugeordnete Geräte** und wählen Sie **Suchen** aus.
3. Geben Sie auf den Registerkarten des Fensters **Suchen** die Kriterien an, nach denen die Client-Geräte gesucht werden sollen, und klicken Sie auf die Schaltfläche **Suchen**.

   Daraufhin werden die Geräte, die den angegebenen Suchkriterien entsprechen, in der Tabelle im unteren Bereich des Fensters **Suchen** angezeigt.

Um Geräte unabhängig davon zu suchen, ob sie einer Administrationsgruppe zugeordnet wurden oder nicht, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver** aus.
2. Wählen Sie im Kontextmenü des Knotens **Suchen** aus.
3. Geben Sie auf den Registerkarten des Fensters **Suchen** die Kriterien an, nach denen die Client-Geräte gesucht werden sollen, und klicken Sie auf die Schaltfläche **Suchen**.

Daraufhin werden die Geräte, die den angegebenen Suchkriterien entsprechen, in der Tabelle im unteren Bereich des Fensters **Suchen** angezeigt.

Außerdem können Sie im Fenster **Suchen** mithilfe der Dropdown-Liste, die sich in der rechten oberen Ecke des Fensters befindet, Administrationsgruppen und sekundäre Administrationsserver suchen. Die Suche nach Administrationsgruppen und sekundären Administrationsservern ist nicht verfügbar, wenn Sie das Fenster **Suchen** aus dem Ordner **Nicht zugeordnete Geräte** geöffnet haben.

Zur Suche nach Geräten können Sie in den Eingabefeldern des Fensters **Suchen** regulären Ausdrücke verwenden.

Die Volltextsuche im Fenster **Suchen** ist verfügbar:

- Auf der Registerkarte **Netzwerk** in dem Abschnitt **Beschreibung**
- Auf der Registerkarte **Hardware**, in den Feldern **Gerät**, **Hersteller** und **Beschreibung**

Suchoptionen für Geräte

Nachfolgend finden Sie Beschreibungen für die Einstellungen zur Suche nach verwalteten Geräten. Die Suchergebnisse werden in der Tabelle im unteren Fensterbereich angezeigt.

Netzwerk

Auf der Registerkarte **Netzwerk** können Sie Suchkriterien für Geräte anhand ihrer Netzwerkdaten konfigurieren:

- **Gerätename oder IP-Adresse**

  Windows-Netzwerkname (NetBIOS-Name) des Geräts oder die IPv4- oder IPv6-Adresse.

- **Windows-Domäne**

  Es werden Geräte angezeigt, die zur angegebenen Windows-Domäne gehören.

- **Administrationsgruppe**

  Es werden Geräte angezeigt, die zur angegebenen Administrationsgruppe gehören.

- **Beschreibung**

  Text, der im Eigenschaftenfenster des Geräts enthalten ist: im Feld **Beschreibung** des Abschnitts **Allgemein**.

Für die Beschreibung eines Textes im Feld **Beschreibung** sind die folgenden Zeichen zulässig:

- Innerhalb eines Wortes:
  - *****. Dieses Zeichen ersetzt beliebige Ausdrücke mit einer beliebigen Zahl von Zeichen.

    Beispiel:

    Für die Beschreibung der Wörter **Server** und **Server-**können Sie die Zeichenfolge **Server*** verwenden.

  - **?.** Dieses Zeichen ersetzt ein beliebiges Symbol.

    Beispiel:

    Für die Beschreibung der Wörter **Regel** oder **Regeln** können Sie die Zeichenfolge **Regel?** verwenden.

    Das Zeichen ***** oder **?** kann nicht als das erste Zeichen in einer Textbeschreibung verwendet werden.

- Zur Verknüpfung mehrerer Wörter:
  - Leerzeichen: Es werden alle Geräte angezeigt, deren Beschreibung ein beliebiges der angegebenen Wörter enthält.

    Beispiel:

    Zur Beschreibung einer Phrase, die entweder das Wort **Sekundär** oder **Virtuell** enthält, können Sie die Zeichenfolge **Sekundär Virtuell** verwenden.

  - **+**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss.

    Beispiel:

    Zur Beschreibung einer Phrase, welche die beiden Wörter **Sekundär** und **Virtuell** enthält, können Sie den Ausdruck **+Sekundär+Virtuell** verwenden.

  - **-**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf.

    Beispiel:

    Zur Beschreibung einer Phrase, die das Wort **Sekundär** enthält, jedoch das Wort **Virtuell** nicht enthalten darf, können Sie den Ausdruck **+Sekundär-Virtuell** verwenden.

  - **"<Textabschnitt>"**: Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein.

    Beispiel:

    Zur Beschreibung einer Phrase, welche die Wortverbindung **Sekundärer Server** enthält, können Sie den Ausdruck **"Sekundärer Server"** verwenden.

- **IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

  Diese Option ist standardmäßig deaktiviert.

- **Verwaltung erfolgt durch anderen Administrationsserver**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Nur die Client-Geräte, die von anderen Administrationsservern verwaltet werden, werden berücksichtigt.
  - **Nein**. Nur die vom selben Administrationsserver verwalteten Client-Geräte, werden berücksichtigt.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Tags

Auf der Registerkarte **Tags** können Sie die Gerätesuche nach Schlüsselworten (Tags) anpassen, die zuvor zu den Beschreibungen der verwalteten Geräte hinzugefügt wurden:

- **Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft**

  Ist die Option aktiviert, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibungen zumindest einer der gewählten Tags vorhanden ist.

  Ist die Option deaktiviert, werden in den Suchergebnissen nur Geräte angezeigt, in deren Beschreibungen alle gewählten Tags vorhanden sind.

  Diese Option ist standardmäßig deaktiviert.

- **Der Tag muss vorhanden sein**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

  Diese Variante ist standardmäßig ausgewählt.

- **Der Tag darf nicht vorhanden sein**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag nicht vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

Active Directory

Auf der Registerkarte **Active Directory** können Sie angeben, dass in der Active Directory-Organisationseinheit (OU) nach Geräten oder Gruppen gesucht werden soll. Sie können auch Geräte aus allen untergeordneten OUs der angegebenen Active Directory-OU in die Auswahl einbeziehen. Um Geräte auszuwählen, geben Sie die folgenden Einstellungen an:

- **Das Gerät befindet sich in einer Active Directory-Organisationseinheit**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Active Directory-Organisationseinheit aufgenommen, das im Eingabefeld angegeben wurde.

  Diese Option ist standardmäßig deaktiviert.

- **Untergeordnete Organisationseinheiten einschließen**

  Wenn die Option aktiviert ist, werden die Geräte aus allen untergeordneten Organisationseinheiten der angegebenen Domänen-Organisationseinheit aufgenommen.

Diese Option ist standardmäßig deaktiviert.

- **Dieses Gerät gehört zu einer Active-Directory-Gruppe**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Active-Directory-Gruppe aufgenommen, die im Eingabefeld angegeben wurde.

  Diese Option ist standardmäßig deaktiviert.

Netzwerkaktivität

Auf der Registerkarte **Netzwerkaktivität** können Sie Suchkriterien für Geräte anhand ihrer Netzwerkaktivitäten konfigurieren:

- **Dieses Gerät ist ein Verteilungspunkt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die als Verteilungspunkte fungieren, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die als Verteilungspunkte fungieren, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Verbindung mit Administrationsserver nicht trennen**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Aktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** aktiviert ist.
  - **Deaktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** deaktiviert ist.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Das Verbindungsprofil wurde gewechselt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Letzte Verbindung mit dem Administrationsserver**

  Mithilfe dieses Kontrollkästchens können Sie ein Kriterium für die Suche von Geräten anhand des Zeitpunkts der letzten Verbindung mit dem Administrationsserver ausführen.

Wenn dieses Kontrollkästchen aktiviert ist, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, während dessen die letzte Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver hergestellt wurde. Bei Auswahl dieser Option werden in die Auswahl Geräte aufgenommen, die dem festgelegten Zeitraum entsprechen.

Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Neue Geräte bei der Netzwerkabfrage erkannt**

  Suche nach neuen Geräten, die während der letzten Tage bei der Netzwerkabfrage gefunden wurden.

  Wenn diese Option aktiviert ist, umfasst die Auswahl nur neue Geräte, die bei einer Gerätesuche während der im Feld **Erkennungszeitraum (Tage)** angegebenen Anzahl von Tagen gefunden wurden.

  Ist die Option deaktiviert, umfasst die Auswahl alle Geräte, die bei einer Gerätesuche gefunden wurden.

  Diese Option ist standardmäßig deaktiviert.

- **Gerät ist sichtbar**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Es werden Geräte in die Auswahl aufgenommen, die momentan im Netzwerk sichtbar sind.
  - **Nein**. Die Anwendung nimmt Geräte in die Auswahl auf, die momentan nicht im Netzwerk sichtbar sind.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Programm

Auf der Registerkarte **Programm** können Sie Suchkriterien für Geräte anhand des ausgewählten verwalteten Programms eingeben:

- **Programmname**

  In der Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl wählen, wenn die Suche anhand des Namens der Kaspersky-Anwendung erfolgt.

  In der Liste sind nur die Anwendungen aufgeführt, für die Verwaltungs-Plug-ins im Administrator-Arbeitsplatz installiert sind.

  Wurde keine Anwendung gewählt, wird kein Kriterium angewandt.

- **Programmversion**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach Versionsnummer der Kaspersky-Anwendung erfolgt.

  Wurde keine Versionsnummer angegeben, wird kein Kriterium angewandt.

- **Name des kritischen Updates**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach dem Namen der Anwendung oder nach der Update-Paketnummer erfolgt.

  Ist dieses Feld leer, wird kein Kriterium angewandt.

- **Letztes Update der Module**

  Mithilfe dieser Option können Sie ein Kriterium für die Suche nach Geräten nach Uhrzeit des letzten Updates der Anwendungsmodule angeben, die auf den Geräten installiert wurden.

  Ist das Kontrollkästchen aktiviert, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, in dem das letzte Update der auf den Geräten installierten Anwendungsmodule ausgeführt wurde.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Gerät wird über Kaspersky Security Center verwaltet**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, die über Kaspersky Security Center verwaltet werden:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn sie über Kaspersky Security Center verwaltet werden.
  - **Nein**. Das Programm nimmt Geräte in die Auswahl auf, wenn sie nicht über Kaspersky Security Center verwaltet werden.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Sicherheitsanwendung ist installiert**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, auf denen eine Sicherheitsanwendung installiert wurde:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn auf ihnen eine Sicherheitsanwendung installiert ist.
  - **Nein**. Die Anwendung nimmt alle Geräte in die Auswahl auf, die keine Sicherheitsanwendung installiert haben.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Betriebssystem

Auf der Registerkarte **Betriebssystem** können Sie die folgenden Suchkriterien anpassen, um Geräte auf Basis des darauf installierten Betriebssystems zu finden:

- **Version des Betriebssystems**

  Ist das Kontrollkästchen aktiviert, können Sie Betriebssysteme in der Liste auswählen. Geräte, auf denen die angegebenen Betriebssysteme installiert sind, werden in die Suchergebnisse aufgenommen.

- **Bitzahl des Betriebssystems**

  In dieser Dropdown-Liste können Sie die Architektur des Betriebssystems auswählen, die vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird (**Unbekannt**, **x86**, **AMD64**, **IA64**). Standardmäßig ist in dieser Liste keine Variante ausgewählt, die Architektur des Betriebssystems ist nicht angegeben.

- **Service Pack-Version des Betriebssystems**

  In diesem Feld können Sie die Service Pack-Version (im Format *X.Y*) des Betriebssystems angeben, die bestimmt, wie die Verschiebungsregel auf das Gerät angewendet wird. Standardmäßig ist keine Version angegeben.

- **Build-Version des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Versionsnummer des Betriebssystems. Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Suche nach allen Versionsnummern mit Ausnahme der angegebenen anpassen.

- **Release-ID des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Release-Identifikator (ID) des Betriebssystems Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-ID haben muss. Sie können auch eine Suche nach allen Release-ID-Nummern mit Ausnahme der angegebenen anpassen.

Gerätestatus

Auf der Registerkarte **Gerätestatus** können Sie die Suchkriterien für Geräte nach dem Gerätestatus des verwalteten Programms angeben:

- **Gerätestatus**

  In dieser Dropdown-Liste können Sie einen Gerätestatus auswählen: *OK*, *Kritisch* oder *Warnung*.

- **Echtzeitschutz-Status**

  In dieser Dropdown-Liste können Sie den Wert für den Status des Echtzeitschutzes auswählen. Geräte mit dem angegebenen Echtzeitschutz-Status werden in die Auswahl aufgenommen.

- **Beschreibung des Gerätestatus**

  In diesem Feld können Sie die Kontrollkästchen für jene Bedingungen aktivieren, auf deren Basis einem Gerät eine der folgenden Statusvarianten zugewiesen werden soll: *OK, Kritisch* oder *Warnung*.

- **Vom Programm bestimmter Gerätestatus**

  In dieser Dropdown-Liste können Sie den Wert für den Status des Echtzeitschutzes auswählen. Geräte mit dem angegebenen Echtzeitschutz-Status werden in die Auswahl aufgenommen.

Schutzkomponenten

Auf der Registerkarte **Schutzkomponenten** können Sie Einstellungen für die Suche nach Client-Geräten nach deren Schutzstatus konfigurieren.

- **Veröffentlichung der Datenbanken**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Veröffentlichungsdatum der Antiviren-Datenbanken. In den Eingabefeldern können Sie den Zeitraum festlegen, anhand dessen die Suche ausgeführt werden soll.

  Diese Option ist standardmäßig deaktiviert.

- **Letzte Virensuche**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Zeitpunkt der letzten Schadsoftware-Untersuchung. In den Eingabefeldern können Sie den Zeitraum festlegen, in dem die Schadsoftware-Untersuchung zum letzten Mal erfolgte.

  Diese Option ist standardmäßig deaktiviert.

- **Gesamtzahl der gefundenen Bedrohungen**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach der Anzahl der gefundenen Viren. In den Eingabefeldern können Sie den unteren und oberen Wert für die Anzahl der gefundenen Viren festlegen.

  Diese Option ist standardmäßig deaktiviert.

Programm-Registry

Auf der Registerkarte **Programm-Registry** können Sie Einstellungen für die Suche von Client-Geräten anhand von installierten Programmen anpassen:

- **Programmname**

  In dieser Dropdown-Liste können Sie einen Anwendungsnamen auswählen. Die Geräte, auf denen diese Anwendung installiert ist, werden in die Auswahl aufgenommen.

- **Programmversion**

  Geben Sie in diesem Eingabefeld die Version der ausgewählten Anwendung ein.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Hersteller der auf dem Gerät installierten Anwendung auswählen.

- **Programm-Status**

  Dropdown-Liste, in der Sie den Status der Anwendung auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen die angegebene Anwendung abhängig vom ausgewählten Status installiert bzw. nicht installiert ist, werden in die Auswahl aufgenommen.

- **Nach Update suchen**

  Wenn diese Option aktiviert ist, erfolgt die Suche anhand der Updatedaten der auf den Geräten installierten Anwendungen. Nachdem Sie das Kontrollkästchen aktiviert haben, ändern sich die Felder **Programmname**, **Programmversion** und **Programm-Status** in **Update-Name**, **Update-Version** und **Status**.

  Diese Option ist standardmäßig deaktiviert.

- **Name der inkompatiblen Sicherheitsanwendung**

  In dieser Dropdown-Liste können Sie Sicherheitsanwendungen von Drittherstellern auswählen. Bei der Suche werden Geräte in die Auswahl aufgenommen, auf denen die ausgewählte Anwendung installiert wurde.

- **Programm-Tag**

  In dieser Dropdown-Liste können Sie ein Anwendungs-Tag auswählen. Alle Geräte, auf denen Programme installiert sind, die den ausgewählten Tag in der Beschreibung haben, werden in die Geräteauswahl aufgenommen.

Hierarchie der Administrationsserver

Aktivieren Sie auf der Registerkarte **Hierarchie der Administrationsserver** das Kontrollkästchen **Daten von sekundären Administrationsservern bis zu dieser Ebene einbeziehen**, falls Sie möchten, dass die auf sekundären Administrationsservern gespeicherten Informationen bei der Suche nach Geräten berücksichtigt werden, und dass Sie im Eingabefeld die Verschachtelungsebene des sekundären Administrationsservers festlegen können, dessen Informationen bei der Gerätesuche berücksichtigt werden sollen. Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

Virtuelle Maschinen

Auf der Registerkarte **Virtuelle Maschinen** können Sie die Einstellungen für die Gerätesuche anpassen, je nachdem, ob diese Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- **Dies ist eine virtuelle Maschine**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Unwichtig**.
  - **Nein**. Die gesuchten Geräte dürfen keine virtuellen Maschinen sein.
  - **Ja**. Die gesuchten Geräte müssen virtuelle Maschinen sein.

- **Typ der virtuellen Maschine**

  In der Dropdown-Liste können Sie den Hersteller der virtuellen Maschine auswählen.

  Die Dropdown-Liste ist verfügbar, wenn die Werte **Ja** oder **Unwichtig** in der Dropdown-Liste **Dies ist eine virtuelle Maschine** gewählt wurden.

- **Teil einer Virtual Desktop Infrastructure (VDI)**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Unwichtig**.
  - **Nein**. Die gesuchten Geräte dürfen kein Teil der Virtual Desktop Infrastructure (VDI) sein.
  - **Ja**. Die gesuchten Geräte müssen Teil der Virtual Desktop Infrastructure (VDI) sein.

Hardware

Auf der Registerkarte **Hardware** können Sie die Suche nach Client-Geräten anhand der darauf installierten Hardware durchführen:

- **Gerät**

  In dieser Dropdown-Liste können Sie einen Einheitentyp auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Namen eines Herstellers der Einheit auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

Im Feld wird die Volltextsuche unterstützt.

- **Beschreibung**

  Beschreibung des Geräts oder der Hardware. Geräte mit der in diesem Feld angegebenen Beschreibung werden in die Auswahl aufgenommen.

  Eine Beschreibung in beliebiger Form kann im Fenster Geräteeigenschaften eingegeben werden. Im Feld wird die Volltextsuche unterstützt.

- **Inventarnummer**

  Hardware mit in diesem Feld angegebener Inventarnummer wird in die Auswahl aufgenommen.

- **Prozessorfrequenz in MHz**

  Frequenzbereich des Prozessors. Geräte mit Prozessoren, die dem Frequenzbereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Virtuelle Prozessorkerne**

  Bereich der Anzahl von virtuellen Cores des Prozessors. Geräte mit Prozessoren, die dem Bereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB)**

  Bereich der Festplattengröße des Geräts. Geräte mit Festplatten, die dem Bereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Speichergröße (MB)**

  Größenbereich des Arbeitsspeichers des Geräts. Geräte mit einem Arbeitsspeicher, der dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

Schwachstellen und Updates

Auf der Registerkarte **Schwachstellen und Updates** können Sie das Kriterium für die Suche nach Geräten gemäß der Quelle der Windows-Updates anpassen:

- **WUA wurde auf den Administrationsserver umgeschaltet**

  In dieser Dropdown-Liste können Sie eine der folgenden Varianten der Suche auswählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte in die Suchergebnisse aufgenommen, die Windows-Updates vom Administrationsserver herunterladen.

  - **Nein**. Bei Auswahl dieser Option werden Geräte in die Ergebnisse aufgenommen, die Windows-Updates von einer anderen Quelle herunterladen.

Benutzer

Auf der Registerkarte **Benutzer** können Sie die Einstellungen für die Suche von Geräten anhand der Benutzerkonten anpassen, die sich am Betriebssystem angemeldet haben.

- **Letzter am System angemeldeter Benutzer**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer als Letzter angemeldet hat.

- **Benutzer, der sich mindestens einmal am System angemeldet hat**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer mindestens einmal im System angemeldet hat.

Statusbeeinflussende Probleme in verwalteten Programmen

Auf der Registerkarte **Statusbeeinflussende Probleme in verwalteten Programmen** können Sie die Suche nach Geräten entsprechend der Statusbeschreibungen anpassen, die vom verwalteten Programm bestimmt werden:

- **Beschreibung des Gerätestatus**

  Sie können die Kontrollkästchen für die Beschreibung der Status der verwalteten Programme aktivieren, bei deren Empfang die Geräte in die Auswahl aufgenommen werden. Wenn Sie einen Status auswählen, der für mehrere Programme aufgelistet ist, haben Sie die Möglichkeit, diesen Status in allen Listen automatisch auszuwählen.

Status der Komponenten in verwalteten Programmen

Auf der Registerkarte **Status der Komponenten in verwalteten Programmen** können Sie die Suche nach Geräten entsprechend des Status der Komponenten anpassen, die sich in verwalteten Programmen befinden:

- **Status des Schutzes vor Datenverlust**

  Suche nach Geräten anhand des Status des "Schutzes vor Datenverlust" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Status des Schutzes der Server für die Zusammenarbeit**

  Suche nach Geräten anhand des Status der Komponente "Schutz der Serverzusammenarbeit" (*Unbekannt*, *Beendet*, *Wird gestartet, Angehalten*, *Wird ausgeführt*, *Fehlgeschlagen*).

- **Status des Antiviren-Schutzes von Mail-Servern**

  Suche nach Geräten anhand des Status des Mail-Server-Schutzes (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Status der Komponente "Endpoint Sensor"**

  Suche nach Geräten anhand des Status der Komponente "Endpoint Sensor" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

Verschlüsselung

- **Verschlüsselung**

  Standard des symmetrischen Algorithmus der Blockverschlüsselung Advanced Encryption Standard (AES). In der Dropdown-Liste können Sie die Länge des Chiffrierschlüssels (56 Bit, 128 Bit, 192 Bit oder 256 Bit) auswählen.

  AES56, *AES128*, *AES192*, *AES256*.

Cloud-Segmente

Auf der Registerkarte **Cloud-Segmente** können Sie die Suche nach der Zugehörigkeit zu Cloud-Segmenten anpassen:

- **Gerät befindet sich in einem Cloud-Segment**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Segment für die Suche auswählen.

  Ist die Option **Inklusive untergeordneter Untergeordnete Objekte einschließen** ebenfalls aktiviert, so wird in allen untergeordneten Objekten des angegebenen Segments eine Suche durchgeführt.

  In die Suchergebnisse werden nur Geräte aus dem ausgewählten Segment aufgenommen.

- **Gerät mithilfe von der API erkannt**

  In der Dropdown-Liste können Sie wählen, ob das Gerät über API gefunden werden soll:

  - **AWS**. Das Gerät wird mithilfe der AWS-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von AWS.
  - **Azure**. Das Gerät wird mithilfe der Azure-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Azure.
  - **Google Cloud.** Das Gerät wird mithilfe der Google-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Google.
  - **Nein**. Das Gerät wird nicht mithilfe der AWS-, Azure- oder Google-API gefunden. Das heißt, es befindet sich entweder außerhalb der Cloud-Umgebung oder es befindet sich in der Cloud-Umgebung, ist aber für die Suche mithilfe API nicht auffindbar.
  - **Kein Wert**. Diese Bedingung trifft nicht zu.

Programmkomponenten

Dieser Abschnitt enthält die Liste der Komponenten jener Anwendungen, in denen entsprechende Verwaltungs-Plug-ins in der Verwaltungskonsole installiert sind.

Im Abschnitt **Programmkomponenten** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status und Versionsnummern der Komponenten festlegen, die sich auf die ausgewählte Anwendung beziehen:

- **Status**

  Suche nach Geräten anhand des Status der Komponente, der von einer Anwendung an den Administrationsserver gesendet wurde. Sie können einen der folgenden Status auswählen: *Keine Daten des Geräts verfügbar*, *Beendet*, *Wird gestartet*, *Angehalten*, *Wird ausgeführt*, *Fehler* oder *Nicht installiert*. Wenn die ausgewählte Komponente der auf einem verwalteten Gerät installierten Anwendung den angegebenen Status aufweist, wird das Gerät bei der Geräteauswahl berücksichtigt.

  Von Anwendungen gesendete Status:

  - *Start*—Die Komponente wird gerade initialisiert.
  - *Wird ausgeführt*–Die Komponente ist aktiviert und funktioniert ordnungsgemäß.
  - *Angehalten*–Die Komponente wird angehalten, z. B. nachdem der Benutzer den Schutz in der verwalteten Anwendung angehalten hat.
  - *Fehler*–Während des Betriebs der Komponente ist ein Fehler aufgetreten.
  - *Beendet*–Die Komponente ist deaktiviert und funktioniert momentan nicht.
  - *Nicht installiert*–Der Benutzer hat die Komponente während der Konfiguration der benutzerdefinierten Installation der Anwendung nicht für die Installation ausgewählt.

  Im Gegensatz zu anderen Status wird der Status *Keine Daten des Geräts verfügbar* nicht von Programmen versendet. Diese Option zeigt, dass die Programme über keine Informationen über den ausgewählten Status der Komponente aufweisen. Dies kann beispielsweise der Fall sein, wenn die ausgewählte Komponente zu keiner der auf dem Gerät installierten Anwendungen gehört oder wenn das Gerät ausgeschaltet ist.

- **Version**

  Suche nach Geräten anhand der Versionsnummer der in der Liste ausgewählten Komponente. Sie können eine Versionsnummer eingeben, beispielsweise `3.4.1.0`, und dann festlegen, ob die ausgewählte Komponente eine gleich, frühere oder spätere Version aufweisen muss. Sie können auch eine Suche nach allen Versionen mit Ausnahme der angegebenen anpassen.

Masken in Zeichenfolgenvariablen verwenden

Für Zeichenfolgenvariablen können Masken verwendet werden. Masken können Sie mit folgenden regulären Ausdrücken erstellen:

- * – beliebige Ausdrücke mit einer Länge von 0 oder mehr Symbolen
- Fragezeichen (?) – ein beliebiges Einzelsymbol.
- [<Bereich>] – Beliebiges einzelnes Zeichen aus einem festgelegten Bereich bzw. der festgelegten Menge.
  Zum Beispiel: [0–9] – Beliebige Ziffer. [abcdef] —Ein beliebiges Zeichen aus a, b, c, d, e oder f.

Reguläre Ausdrücke in der Suchzeile verwenden

Zur Suche nach einzelnen Wörtern oder Symbolen können Sie die folgenden regulären Ausdrücke in der Suchzeile verwenden:

- *. Ersetzt eine Folge einer beliebigen Anzahl von Zeichen. Zur Suche nach den Wörtern "Server", oder "Server-" geben Sie beispielsweise in der Suchzeile den Ausdruck `Server*` ein.
- ?. Dieses Zeichen ersetzt ein beliebiges Symbol. Zur Suche nach den Wörtern "Fenstern" oder "Fensters" geben Sie beispielsweise den Ausdruck `Fenster?` in der Suchzeile ein.

  > Der Text in der Suchzeile darf nicht mit dem Symbol "?" anfangen.

- [<Intervall>]. Ersetzt ein Zeichen aus dem festgelegten Bereich bzw. der festgelegten Menge. Zur Suche nach einer beliebigen Ziffer geben Sie beispielsweise den Ausdruck `[0-9]` in der Suchzeile ein. Zur Suche nach einem der folgenden Symbole a, b, c, d, e, f geben Sie den Ausdruck `[abcdef]` in der Suchzeile ein.

Zur Volltextsuche können Sie die folgenden regulären Ausdrücke in der Suchzeile verwenden:

- Leerzeichen: Als Ergebnis werden alle Geräte angezeigt, deren Beschreibung ein beliebiges der angegebenen Wörter enthält. Zur Suche nach einer Phrase, die das Wort "Sekundär" oder "Virtuell" (bzw. beide Wörter) enthält, geben Sie beispielsweise den Ausdruck `Sekundär Virtuell` in der Suchzeile ein.
- Zeichen "plus" (+), AND oder &&. Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss. Zur Suche nach einer Phrase, die das Wort "Sekundär" und das Wort "Virtuell" enthält, können Sie beispielsweise die folgenden Ausdrücke in der Suchzeile eingeben: `+Sekundär+Virtuell`, `Sekundär AND Virtuell`, `Sekundär && Virtuell`.
- OR oder ||. Zwischen den Wörtern stehend bedeutet dieses Zeichen, dass eines der Wörter im Text vorhanden sein muss. Zur Suche nach einer Phrase, die das Wort "Sekundär" oder das Wort "Virtuell" enthält, können Sie beispielsweise die folgenden Ausdrücke in der Suchzeile eingeben: `Sekundär OR Virtuell`, `Sekundär || Virtuell`.
- Zeichen "minus" (-). Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf. Zur Suche nach einer Phrase, in der das Wort "Sekundär" vorhanden sein und das Wort "Virtuell" fehlen muss, geben Sie beispielsweise den Ausdruck `+Sekundär-Virtuell` in der Suchzeile ein.
- `"< Textabschnitt >"`. Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein. Zur Suche nach einer Phrase, in der die Wortkombination "Sekundärer Server" vorhanden ist, geben Sie beispielsweise den Ausdruck `" Sekundärer Server "` in der Suchzeile ein.

Die Volltextsuche ist in den folgenden Filterblöcken verfügbar:

- Filterblock der Ereignisliste nach Spalten **Ereignis** und **Beschreibung**
- Filterblock für Benutzerkonten nach Spalte **Name**
- Filterblock für die Programm-Registry nach Spalte **Name**, wenn im Block **In der Liste anzeigen** das Filterkriterium **nicht gruppiert** ausgewählt ist

Listen aus Dialogfenstern exportieren

In den Dialogfenstern des Programms können Sie Objektlisten in Textdateien exportieren.

Objektlisten können nur für die Abschnitte des Dialogfensters exportiert werden, in welchen die Schaltfläche **In Datei exportieren** vorhanden ist.

Einstellungen für Aufgaben

In diesem Abschnitt werden alle Einstellungen für Aufgaben in Kaspersky Security Center aufgelistet.

Allgemeine Aufgabeneinstellungen

Dieser Abschnitt enthält die Einstellungen, die Sie für Aufgaben anzeigen und konfigurieren können. Die Liste der verfügbaren Einstellungen hängt von der Aufgabe ab, die Sie konfigurieren.

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- Neustart-Einstellungen des Betriebssystems:
  - **Gerät nicht neu starten**

    Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

  - **Gerät neu starten**

    Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

  - **Benutzer fragen**

    Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

    Diese Option ist standardmäßig ausgewählt.

- **Aufforderung regelmäßig wiederholen alle (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neustart nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Programmen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

- Zeitplaneinstellungen für Aufgaben:

  Die Arten des Zeitplans können je nach Aufgabe variieren.

  - **Einstellung Start nach Zeitplan:**

    - **Alle n Stunden**

      Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

      Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

    - **Alle n Tage**

      Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

      Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

    - **Alle n Minuten**

      Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

      Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Einmal**

  Die Aufgabe wird einmal zum angegebenen Datum und zur angegebenen Uhrzeit ausgeführt (standardmäßig entspricht dies dem Tag, an dem die Aufgabe erstellt wurde).

- **Sofort**

  Die Aufgabe wird nach dem Speichern der Einstellungen umgehend ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Nach dem Download von Updates in die Datenverwaltung**

  Die Aufgabe wird gestartet, nachdem Updates in die Datenverwaltung heruntergeladen wurden. Sie können diesen Zeitplan beispielsweise zur Suchen nach Suche nach Schwachstellen und erforderlichen Updates verwenden.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

- Geräte, denen die Aufgabe zugewiesen wird:

  - **Geräte auswählen, die vom Administrationsserver erkannt wurden**

    Die Aufgabe wird einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

    Sie können diese Option beispielsweise für eine Aufgabe zur Installation des Administrationsagenten auf nicht zugeordneten Geräten verwenden.

  - **Geräteadressen manuell angeben oder aus Liste importieren**

    Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

    Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

  - **Aufgabe einer Geräteauswahl zuweisen**

    Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

    Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

  - **Aufgabe einer Administrationsgruppe zuweisen**

    Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

    Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

    Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

- Benutzerkonto-Einstellungen:

  - **Standardbenutzerkonto**

    Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

    Diese Variante ist standardmäßig ausgewählt.

  - **Benutzerkonto festlegen**

    Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

  - **Benutzerkonto**

    Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

- **Kennwort**

  Kennwort des Benutzerkontos, unter dem die Aufgabe ausgeführt wird.

Wenn der Administrationsagent nicht auf Ihrem Zielgerät installiert ist, müssen Sie das Benutzerkonto angeben, das auf dem Zielgerät für den Zugriff auf die Freigabe "admin$" verwendet werden soll. Das angegebene Konto dient nur dazu, die Daten auf Ihr Gerät zu kopieren. Wenn der Administrationsagent auf Ihrem Zielgerät installiert ist, werden die Daten durch den Administrationsagenten kopiert und Sie müssen beim Erstellen der Aufgabe kein Benutzerkonto angeben.

Einstellungen, die nach der Aufgabenerstellung festgelegt werden

Sie können die folgenden Einstellungen erst festlegen, nachdem eine Aufgabe erstellt wurde.

- Einstellungen der Gruppenaufgabe:

  - **Auf Untergruppen verteilen**

    Diese Option ist nur in den Einstellungen der Gruppenaufgaben verfügbar.

    Wenn diese Option aktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe die folgenden Objekte:

    - Die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.
    - Die Administrationsgruppen, die der ausgewählten Administrationsgruppe entsprechend der Gruppenhierarchie auf beliebiger Ebene untergeordnet sind.

    Wenn diese Option deaktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe nur die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.

    Diese Option ist standardmäßig aktiviert.

  - **An sekundäre und virtuelle Administrationsserver verteilen**

    Wenn diese Option aktiviert ist, wird die Aufgabe, die auf dem primären Administrationsserver wirksam ist, auch auf den sekundären Administrationsservern (einschließlich virtuellen) angewendet. Wenn auf dem sekundären Administrationsserver bereits eine Aufgabe des gleichen Typs existiert, werden auf dem sekundären Administrationsserver beide Aufgaben angewendet – die bestehende und die vom primären Administrationsserver übernommene.

    Diese Option ist nur verfügbar, wenn die Option **Auf Untergruppen verteilen** aktiviert ist.

    Diese Option ist standardmäßig deaktiviert.

- Erweiterte Zeitplaneinstellungen:

  - **Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren (Min.)**

    Das Betriebssystem auf dem Gerät startet zum angegebenen Zeitpunkt, bevor die Aufgabe gestartet wird. Standardmäßig beträgt die Zeitspanne fünf Minuten.

    Aktivieren Sie diese Option, wenn Sie möchten, dass die Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich ausgeführt wird, einschließlich jener Geräte, die ausgeschaltet sind, wenn die Aufgabe gestartet werden soll.

    Wenn das Gerät nach Abschluss der Aufgabe automatisch ausgeschaltet werden soll, aktivieren Sie die Option **Geräte nach Abschluss der Aufgabe herunterfahren**. Die Option befindet sich im selben Fenster.

    Diese Option ist standardmäßig deaktiviert.

- **Geräte nach Abschluss der Aufgabe herunterfahren**

  Sie können diese Option beispielsweise für eine Aufgabe zur Installation von Updates aktivieren, die Updates für Client-Geräte jeden Freitag nach Geschäftsschluss installiert und diese Geräte dann über das Wochenende abschaltet.

  Diese Option ist standardmäßig deaktiviert.

- **Aufgabe anhalten, wenn sie länger ausgeführt wird als (Min.)**

  Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

- Benachrichtigungseinstellungen:

  - Block **Ereignisdaten der Aufgabe speichern**:

    - **Auf dem Administrationsserver für (Tage)**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich beziehen, werden auf dem Administrationsserver während der festgelegten Anzahl an Tagen gespeichert. Wenn diese Zeitspanne abgelaufen ist, werden die Informationen vom Administrationsserver gelöscht.

      Diese Option ist standardmäßig aktiviert.

    - **Im System-Ereignisprotokoll des Geräts speichern**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe beziehen, werden lokal im Windows Ereignisprotokoll jedes Client-Geräts gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - **Im System-Ereignisprotokoll des Administrationsservers speichern**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich beziehen, werden zentral im Windows Ereignisprotokoll des Betriebssystems des Administrationsservers gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - **Alle Ereignisse speichern**

      Wenn diese Option ausgewählt ist, werden alle Ereignisse, die sich auf die Aufgabe beziehen, in den Ereignisprotokollen gespeichert.

    - **Ereignisse in Bezug auf Aufgabenfortschritt speichern**

      Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

- **Nur die Ergebnisse der Aufgabenausführung speichern**

  Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Ergebnisse der Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

- **Den Administrator über Ergebnisse der Aufgabenausführung benachrichtigen**

  Sie können die Methoden auswählen, über die Administratoren Benachrichtigungen über Ergebnisse der Aufgabenausführung erhalten: per E-Mail, mit SMS und durch Start einer ausführbaren Datei. Um die Benachrichtigungen zu konfigurieren, klicken Sie auf den Link **Einstellungen**.

  Standardmäßig sind alle Methoden der Zustellung von Benachrichtigungen deaktiviert.

- **Nur über Fehler benachrichtigen**

  Wenn diese Option aktiviert ist, werden Administratoren nur dann benachrichtigt, wenn die Aufgabenausführung mit einem Fehler beendet wird.

  Wenn diese Option deaktiviert ist, werden Administratoren nach jeder Aufgabenausführung benachrichtigt.

  Diese Option ist standardmäßig aktiviert.

- Sicherheitseinstellungen

- Einstellungen für den Gültigkeitsbereich

  Abhängig davon, wie der Gültigkeitsbereich der Aufgabe bestimmt wird, sind die folgenden Einstellungen verfügbar:

  - **Geräte**

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Administrationsgruppe bestimmt wird, können Sie diese Gruppe anzeigen. Hier sind keine Änderungen möglich. Sie können aber **Ausschlüsse vom Gültigkeitsbereich der Aufgabe** festlegen.

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Liste von Geräten bestimmt wird, können Sie diese Liste ändern, indem Sie Geräte hinzufügen und entfernen.

  - **Geräteauswahl**

    Sie können die Geräteauswahl ändern, für welche die Aufgabe übernommen wird.

  - **Ausschlüsse vom Gültigkeitsbereich der Aufgabe**

    Sie können Gruppen von Geräten festlegen, für welche die Aufgabe nicht angewendet wird. Gruppen, die ausgeschlossen werden sollen, können sich nur den Untergruppen der Administrationsgruppe befinden, für welche die Aufgabe übernommen wird.

- **Revisionsverlauf**

Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- **Quellen der Updates**

  Als Update-Quelle für den Administrationsserver können die folgenden Ressourcen verwendet werden:

  - Kaspersky-Update-Server

    HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen. Standardmäßig verwendet der Administrationsserver zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können Administrationsserver so einrichten, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

    Standardmäßig ausgewählt.

  - Primärer Administrationsserver

    Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.

  - Lokaler Ordner oder Netzwerkordner

    Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Ein Netzwerkordner kann ein FTP- oder HTTP-Server oder eine SMB-Freigabe sein. Für Netzwerkordner, die eine Authentifizierung erfordern, wird nur das SMB-Protokoll unterstützt. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

    > Ein FTP- oder HTTP-Server oder ein Netzwerkordner, der von einer Update-Quelle verwendet wird, muss eine Ordnerstruktur (mit Updates) enthalten, die der Struktur entspricht, die bei Verwendung der Kaspersky-Update-Server erstellt wurde.

- **Sonstige Einstellungen**

  Update der sekundären Administrationsserver erzwingen

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Update-Aufgaben auf den sekundären Administrationsservern sobald neue Updates heruntergeladen werden. Update-Aufgaben werden unter Verwendung der Update-Quellen gestartet, die in den Aufgabeneigenschaften auf den sekundären Administrationsservern konfiguriert ist.

  Wenn diese Option deaktiviert ist, werden die Update-Aufgaben auf den sekundären Administrationsservern gemäß ihren Zeitplänen gestartet.

  Diese Option ist standardmäßig deaktiviert.

  Heruntergeladene Updates in zusätzliche Ordner kopieren

  Nachdem der Administrationsserver Updates empfängt, kopiert er sie in die angegebenen Ordner. Verwenden Sie diese Option, wenn Sie die Verteilung von Updates in Ihrem Netzwerk manuell verwalten möchten.

Sie können diese Option beispielsweise in der folgenden Situation verwenden: Das Netzwerk Ihres Unternehmens besteht aus mehreren unabhängigen Subnetzen, wobei Geräte in den einzelnen Subnetzen über keinen Zugriff auf andere Subnetze verfügen. Allerdings haben Geräte in allen Teilnetzen Zugriff auf eine gemeinsame Netzwerkfreigabe. In diesem Fall müssen Sie den Administrationsserver in einem der Subnetze einrichten, um Updates von den Kaspersky-Update-Servern herunterzuladen. Aktivieren Sie diese Option und geben Sie dann diese Netzwerkfreigabe an. Geben Sie bei heruntergeladenen Updates der Repository-Aufgaben für andere Administrationsserver die gleiche Netzwerkfreigabe wie für die Update-Quelle an.

Wenn Sie auswählen, dass die Updates in einen lokalen Ordner kopiert werden sollen, müssen Sie einen Ordner auf dem Gerät mit dem installierten Administrationsserver angeben. Der Pfad des Ordners hängt vom Betriebssystem auf dem Gerät ab. Da sich der lokale Ordner auf einem Linux-basierten Administrationsserver befindet, müssen Sie den POSIX-Pfad angeben. Beispiel: /Pfad/zum/Verzeichnis.

Wenn Sie einen Netzwerkordner auswählen, der sich auf einem Linux-Administrationsserver befindet, müssen Sie vorher durch das Mounten des Ordners sicherstellen, dass von dem Gerät mit installiertem Administrationsserver auf den Netzwerkordner zugegriffen werden kann. Der Zugriff auf den Ordner erfolgt über das SMB-Protokoll.

Diese Option ist standardmäßig deaktiviert.

Update der Geräte und sekundären Administrationsserver bis Abschluss des Kopierens nicht erzwingen

Die Aufgaben zum Herunterladen von Updates auf Client-Geräte und sekundäre Administrationsserver werden erst gestartet, nachdem diese Updates vom Update-Hauptordner in die zusätzlichen Ordner kopiert wurden.

Diese Option muss aktiviert sein, wenn Client-Geräte und sekundäre Administrationsserver Updates von zusätzlichen Netzwerkordnern herunterladen.

Diese Option ist standardmäßig deaktiviert.

Einstellungen, die nach der Aufgabenerstellung festgelegt werden

Sie können die folgenden Einstellungen erst festlegen, nachdem eine Aufgabe erstellt wurde.

- Abschnitt **Einstellungen**, Block **Inhalt der Updates**

  Diff-Dateien herunterladen

  Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

  Diese Option ist standardmäßig deaktiviert.

- Bereich **Update-Prüfung**

  Update-Prüfung vor der Verteilung ausführen

  Der Administrationsserver lädt Updates von der Quelle herunter, speichert sie in einer temporären Datenverwaltung und führt die Aufgabe aus, die im Feld **Aufgabe zur Update-Prüfung** angegeben wurde. Wenn die Aufgabe erfolgreich beendet wird, werden die Updates von der temporären Datenverwaltung in einen freigegebenen Ordner auf dem Administrationsserver kopiert und anschließend auf alle Geräte verteilt, für die der Administrationsserver als Update-Quelle dient (Aufgaben mit dem Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** werden gestartet). Die Aufgabe zum Download von Updates in die Datenverwaltung wird erst nach Abschluss der Aufgabe zur *Update-Prüfung* beendet.

  Diese Option ist standardmäßig deaktiviert.

  Aufgabe zur Update-Prüfung

  Diese Aufgabe überprüft heruntergeladene Updates, bevor sie an alle Geräte verteilt werden, für die der Administrationsserver als Update-Quelle dient.

In diesem Feld können Sie die von Ihnen zuvor erstellte Aufgabe zur *Update-Prüfung* angeben. Alternativ können Sie eine neue Aufgabe zur *Update-Prüfung* erstellen.

Einstellungen der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- **Quellen der Updates**

  Als Update-Quelle für den Verteilungspunkt können die folgenden Ressourcen verwendet werden:

  - Kaspersky-Update-Server

    HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen.

    Diese Variante ist standardmäßig festgelegt.

  - Primärer Administrationsserver

    Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.

  - Lokaler Ordner oder Netzwerkordner

    Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Ein Netzwerkordner kann ein FTP- oder HTTP-Server oder eine SMB-Freigabe sein. Für Netzwerkordner, die eine Authentifizierung erfordern, wird nur das SMB-Protokoll unterstützt. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

    > Ein FTP- oder HTTP-Server oder ein Netzwerkordner, der von einer Update-Quelle verwendet wird, muss eine Ordnerstruktur (mit Updates) enthalten, die der Struktur entspricht, die bei Verwendung der Kaspersky-Update-Server erstellt wurde.

- **Sonstige Einstellungen → Ordner zum Speichern von Updates**

  Der Pfad zum angegebenen Ordner, in dem die bezogenen Updates gespeichert werden. Sie können den Pfad des angegebenen Ordners in die Zwischenablage kopieren. Für eine Gruppenaufgabe können Sie den Pfad eines angegebenen Ordners nicht ändern.

Einstellungen, die nach der Aufgabenerstellung festgelegt werden

Sie können die folgende Einstellung im Abschnitt **Einstellungen** des Blocks **Inhalt der Updates** erst angeben, nachdem die Aufgabe erstellt wurde.

Diff-Dateien herunterladen

Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

Diese Option ist standardmäßig deaktiviert.

Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

  Wenn Kaspersky Security Center nach Schwachstellen und Updates sucht, verwendet das Programm die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

  Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und Updates für Drittanbieter-Apps haben.

  Diese Option ist standardmäßig aktiviert.

  Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

  - **Mit dem Update-Server verbinden, um Daten zu aktualisieren**

    Der Windows-Update-Agent auf einem verwalteten Gerät stellt eine Verbindung zur Quelle für Microsoft-Updates her. Die folgenden Server können als Quelle für Microsoft-Updates dienen:

    - Kaspersky Security Center Administrationsserver (siehe Einstellungen der Richtlinie des Administrationsagenten)
    - Windows Server mit Microsoft Windows Server Update Services (WSUS), das in Ihrem Unternehmensnetzwerk bereitgestellt wurde
    - Microsoft-Update-Server

    Wenn diese Option aktiviert ist, stellt der Windows-Update-Agent auf einem verwalteten Gerät eine Verbindung zur Quelle für Microsoft-Updates her, um die Informationen über geeignete Microsoft-Windows-Updates zu aktualisieren.

    Wenn diese Option deaktiviert ist, verwendet der Windows-Update-Agent auf einem verwalteten Gerät die Informationen über geeignete Microsoft Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden.

    Das Herstellen einer Verbindung zur Quelle für Microsoft-Updates kann ressourcenaufwendig sein. Sie können diese Option deaktivieren, wenn Sie in einer anderen Aufgabe oder in den Eigenschaften der Administrationsagenten-Richtlinie im Abschnitt **Software-Updates und Schwachstellen** eine regelmäßige Verbindung zu dieser Update-Quelle festgelegt haben. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um eine Überlastung des Servers zu vermeiden.

    Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, die in den Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Der Windows-Update-Agent auf einem verwalteten Gerät stellt nur unter den folgenden Bedingungen eine Verbindung zum Update-Server her, um Updates zu erhalten: Die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** in den Eigenschaften der Aufgabe zum *Suche nach Schwachstellen und erforderlichen Updates* ist aktiviert und die Option **Modus für die Suche nach Windows-Updates** steht in den Einstellungen der Administrationsagent-Richtlinie auf **Aktiv**.

- Wenn Sie den Administrationsagenten nicht benötigen, um während der Ausführung der Aufgabe *Untersuchung auf Schwachstellen* eine Verbindung zur Microsoft Windows-Update-Quelle herzustellen und Updates herunterzuladen, können Sie die Option **Modus für die Suche nach Windows-Updates** auf **Offline** setzen, wobei die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert bleiben muss. Auf diese Weise können Sie Ressourcen sparen und zuvor abgerufene Windows-Updates verwenden, um nach Schwachstellen zu suchen. Sie können den passiven Modus verwenden, wenn Sie das Abrufen von Microsoft Windows-Updates auf eine andere Art konfigurieren. Wenn das Abrufen von Microsoft Windows-Updates jedoch nicht auf eine andere Art konfiguriert ist, setzen Sie die Option **Modus für die Suche nach Windows-Updates** nicht auf **Offline**, da in diesem Fall keine Informationen über Updates abgerufen werden.

- Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert), wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** gesetzt ist, fragt Kaspersky Security Center keine Informationen über Updates ab.

- **Nach Schwachstellen und Updates von Drittherstellern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Security Center in der Windows-Registrierung und den unter Geben Sie Pfade für eine zusätzliche Suche nach Programmen im Dateisystem an **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für fremde Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

  Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps haben.

  Diese Option ist standardmäßig aktiviert.

  - **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an**

    Die Ordner, in denen Kaspersky Security Center nach Drittanbieter-Apps sucht, für die ein Schließen von Schwachstellen und eine Update-Installation erforderlich ist. Sie können Systemvariable verwenden.

    Legen Sie die Ordner fest, in denen Programme installiert sind. Standardmäßig enthält die Liste die Systemordner, in denen die meisten Programme installiert sind.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

Erforderliche Updates installieren und Schwachstellen schließen

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- **Regeln für die Installation von Updates festlegen**

  Diese Regeln werden für die Installation von Updates auf Client-Geräten übernommen. Wenn keine Regeln festgelegt sind, wird die Aufgabe nicht ausgeführt. Informationen über Vorgänge mit Regeln finden Sie unter Regeln zur Installation von Updates.

- **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen**

  Ist diese Option aktiviert, so werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Andernfalls werden Updates nach einem Zeitplan installiert.

  Verwenden Sie diese Option, wenn die Installation von Updates die Geräteleistung beeinträchtigen könnte.

  Diese Option ist standardmäßig deaktiviert.

- **Erforderliche Systemkomponenten installieren**

  Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

  Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

  Diese Option ist standardmäßig deaktiviert.

- **Installation einer neuen Programmversion beim Update zulassen**

  Ist diese Option aktiviert, so werden Updates erlaubt, wenn sie zur Installation einer neuen Version einer Softwareanwendung führen.

  Wenn diese Option deaktiviert ist, wird die Software nicht aktualisiert. Sie können dann neue Versionen der Software manuell oder über eine andere Aufgabe installieren. Sie können diese Option beispielsweise verwenden, wenn die Infrastruktur Ihres Unternehmens nicht von einer neuen Softwareversion unterstützt wird oder wenn Sie ein Update in einer Testinfrastruktur überprüfen möchten.

Diese Option ist standardmäßig aktiviert.

> Aktualisieren einer Anwendung kann zu Fehlern bei abhängigen Anwendungen führen, die auf Client-Geräten installiert sind.

- **Updates auf das Gerät herunterladen, ohne sie zu installieren**

  Wenn diese Option aktiviert ist, lädt die Anwendung Updates auf das Gerät herunter, installiert sie jedoch nicht automatisch. Sie können die heruntergeladenen Updates dann manuell installieren.

  Microsoft-Updates werden in den Windows-Systemspeicher heruntergeladen. Updates für Drittanbieter-Anwendungen (Anwendungen, die von den Software-Herstellern Kaspersky oder Microsoft stammen) werden in den Ordner heruntergeladen, der im Feld **Updates herunterladen nach** angegeben ist.

  Wenn diese Option deaktiviert ist, werden die Updates automatisch auf dem Gerät installiert.

  Diese Option ist standardmäßig deaktiviert.

  - **Updates herunterladen nach**

    Dieser Ordner wird verwendet, um Updates für Drittanbieter-Anwendungen (Anwendungen, die nicht von den Software-Herstellern Kaspersky oder Microsoft stammen) herunterzuladen.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

  - **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

    Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

Einstellungen, die nach der Aufgabenerstellung festgelegt werden

Sie können die folgenden Einstellungen aus den folgenden Abschnitten erst festlegen, nachdem eine Aufgabe erstellt wurde. Eine vollständige Beschreibung der Aufgabeneinstellungen finden Sie unter Allgemeine Aufgabeneinstellungen.

- **Allgemein**. In diesem Abschnitt werden allgemeine Informationen zur Aufgabe angezeigt. Außerdem können Sie angeben, auf welchen Geräten die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* angewendet werden soll:

  - **Auf Untergruppen verteilen**

    Diese Option ist nur in den Einstellungen der Gruppenaufgaben verfügbar.

    Wenn diese Option aktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe die folgenden Objekte:

    - Die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.
    - Die Administrationsgruppen, die der ausgewählten Administrationsgruppe entsprechend der Gruppenhierarchie auf beliebiger Ebene untergeordnet sind.

    Wenn diese Option deaktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe nur die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.

    Diese Option ist standardmäßig aktiviert.

  - **An sekundäre und virtuelle Administrationsserver verteilen**

    Wenn diese Option aktiviert ist, wird die Aufgabe, die auf dem primären Administrationsserver wirksam ist, auch auf den sekundären Administrationsservern (einschließlich virtuellen) angewendet. Wenn auf dem sekundären Administrationsserver bereits eine Aufgabe des gleichen Typs existiert, werden auf dem sekundären Administrationsserver beide Aufgaben angewendet – die bestehende und die vom primären Administrationsserver übernommene.

    Diese Option ist nur verfügbar, wenn die Option **Auf Untergruppen verteilen** aktiviert ist.

    Diese Option ist standardmäßig deaktiviert.

- Zu installierende Updates

  Im Abschnitt **Zu installierende Updates** können Sie die Liste der bei der Aufgabe installierten Updates angezeigt. Es werden nur Updates angezeigt, die den übernommenen Aufgabeneinstellungen entsprechen.

- Testinstallation von Updates:

  - **Nicht untersuchen**. Wählen Sie diese Option aus, wenn Sie keine Testinstallation von Updates ausführen möchten.
  - **Untersuchung auf den gewählten Geräten durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf bestimmten Geräten prüfen möchten. Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie die Geräte aus, auf denen Sie die Testinstallation von Updates ausführen möchten.

- **Untersuchung auf den Geräten in der angegebenen Gruppe durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf einer Gruppe von Geräten prüfen möchten. Geben Sie im Feld **Geben Sie eine Testgruppe an** eine Gruppe von Geräten an, auf denen eine Testinstallation ausgeführt werden soll.

- **Untersuchung für den angegebenen Prozentsatz an Geräten durchführen**. Wählen Sie diese Option aus, wenn Sie die Untersuchung der Updates auf einem Teil der Geräte durchführen möchten. Geben Sie im Feld **Prozentsatz der Testgeräte von der gesamten Anzahl von Zielgeräten** den Prozentanteil der Geräte an, auf denen Sie die Testinstallation von Updates ausführen möchten.

Globale Liste der Subnetze

Dieser Abschnitt bietet Informationen über die globale Liste der Subnetze, die Sie in den Regeln verwenden können.

Um Informationen über Subnetze Ihres Netzwerks zu speichern, können Sie für jeden Administrationsserver, den Sie verwenden, eine globale Liste der Subnetze einrichten. Diese Liste hilft Ihnen dabei Paare {IP-Adresse, Maske} und physikalische Einheiten wie Filialen übereinzustimmen. Sie können Subnetze aus dieser Liste in den Netzwerkregeln und Einstellungen verwenden.

Hinzufügen von Subnetzen zur globalen Liste der Subnetze

Sie können Subnetz mit ihren Beschreibungen zur globalen Liste der Subnetze hinzufügen.

Um ein Subnetz zur globalen Liste der Subnetze hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten des erforderlichen Administrationsservers aus.

2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.

3. Wählen Sie im nächsten Fenster **Eigenschaften** im Bereich **Abschnitte** den Punkt **Liste der globalen Subnetze** aus.

4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Neues Subnetz** wird geöffnet.

5. Füllen Sie die folgenden Felder aus:

   - **Allgemeine Einstellungen**

     Die Subnetz-IP-Adresse für das Subnetz, das Sie hinzufügen.

   - **Subnetzmaske**

     Die Subnetzmaske für das Subnetz, das Sie hinzufügen.

   - **Name**

     Der Name des Subnetzes. Dieser muss innerhalb der globalen Liste der Subnetze eindeutig sein. Wenn Sie einen Namen eingeben, der bereits existiert, wird ein Index hinzugefügt, beispielsweise ~~1,~~2.

- **Beschreibung**

  Die Beschreibung kann zusätzliche Informationen über die Filiale enthalten, in der sich da Subnetz befindet. Dieser Text wird in allen Listen angezeigt, in denen dieses Subnetz vorhanden ist, beispielsweise in der Liste mit Regeln zur Begrenzung des Datenverkehrs.

  Dieses Feld ist kein Pflichtfeld und kann leer gelassen werden.

6. Klicken Sie auf die Schaltfläche **OK**.

Das Subnetz wird in der Liste der Subnetze angezeigt.

Anzeigen und Ändern von Subnetzeigenschaften in der globalen Liste der Subnetze

Sie können die Eigenschaften von Subnetzen in der globalen Liste der Subnetze anzeigen und ändern.

Um Eigenschaften eines Subnetzes in der globalen Liste der Subnetze anzuzeigen oder zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten des erforderlichen Administrationsservers aus.
2. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
3. Wählen Sie im nächsten Fenster **Eigenschaften** im linken Bereich **Abschnitte** die Option **Liste der globalen Subnetze** aus.
4. Klicken Sie in der Liste auf das gewünschte Subnetz.
5. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Neues Subnetz** wird geöffnet.
6. Falls notwendig, ändern Sie die Einstellungen des Subnetzes.
7. Klicken Sie auf die Schaltfläche **OK**.

Wenn Sie Änderungen gemacht haben, werden diese gespeichert.

Administrationsagent für Windows, Linux und macOS: Vergleich

Die Verwendung des Administrationsagenten hängt vom Betriebssystem des Geräts ab. Die Einstellungen für die Richtlinie des Administrationsagenten und das Installationspaket unterscheiden sich ebenfalls in Abhängigkeit vom Betriebssystem. In der folgenden Tabelle werden für den Administrationsagenten die Funktionen und Verwendungsszenarien für Windows-, macOS- und Linux-Betriebssysteme verglichen.

Funktion des Administrationsagenten	Windows	Linux	macOS
Installation			
Automatisches Erzeugen des Installationspakets für den Administrationsagenten nach der Installation von Kaspersky Security Center	✓	–	–
Installation im erzwungen Modus mithilfe der entsprechenden Optionen in der Aufgabe zur Remote-Installation von Kaspersky Security Center	✓	✓	✓
Installation mittels an die Gerätebenutzer geschickten Link, der zu den von Kaspersky Security Center erzeugten autonomen Pakete führt	✓	✓	✓
Installation mittels Klonen eines Festplatten-Images mit Betriebssystem und installiertem Administrationsagenten unter Verwendung von Tools, die durch Kaspersky Security Center für die Arbeit mit Laufwerks-Images bereitgestellten werden	✓	–	–
Installation mittels Klonen eines Festplatten-Images mit Betriebssystem und installiertem Administrationsagenten unter Verwendung von Drittanbieter -Tools	✓	✓	✓
Installation mittels Drittanbietern-Tools zur Remote-Installation von Anwendungen	✓	✓	✓
Installation durch manuelles Starten der Installer der Anwendungen auf den Geräten	✓	✓	✓
Installation des Administrationsagenten im Silent-Modus	✓	✓	✓
Client-Gerät manuell mit Administrationsserver verbinden. "klmover"-Tool	✓	✓	✓
Automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center	✓	✓	–
Automatische Verteilung von Schlüsseln	✓	✓	✓
Erzwungene Synchronisierung	✓	✓	✓ Außer Push-Server
Verteilungspunkt			
Verwendung als Verteilungspunkt	✓	✓	✓

Funktion des Administrationsagenten	Windows	Linux	macOS
Berechnung der Anzahl und Konfiguration der Verteilungspunkte	✓	✓ Ohne die Verwendung von Network Location Awareness (NLA).	✓ Ohne die Verwendung von Network Location Awareness (NLA).
Netzwerkabfrage	✓ • Windows-Netzwerkabfrage • IP-Bereiche abfragen • Abfrage des Domänencontrollers (Microsoft Active Directory)	✓ • IP-Bereiche abfragen • Zeroconf-Abfrage • Abfrage des Domänencontrollers (Microsoft Active Directory, Samba 4 Active Directory)	–
KSN-Proxy-Service auf dem Verteilungspunkt ausführen	✓	✓	–
Herunterladen von Updates über Kaspersky-Update-Server in die Datenverwaltungen der Verteilungspunkte, welche wiederum die Updates an verwaltete Geräte verteilen	✓	✓	– (Wenn ein oder mehrere Geräte, die unter Linux oder macOS laufen, in den Bereich der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte fallen, schließt die Aufgabe mit dem Status "Fehlgeschlagen" ab, selbst wenn sie auf allen Windows-Geräten erfolgreich abgeschlossen wurde)
Push-Installation von Anwendungen	✓	Eingeschränkt: Es ist nicht möglich, mithilfe von Linux-Verteilungspunkten eine Push-Installation auf Windows-Geräten durchzuführen.	Eingeschränkt: Es ist nicht möglich, mithilfe von macOS-Verteilungspunkten eine Push-Installation auf Windows-Geräten durchzuführen.
Verwendung als Push-Server	✓	✓	–
Umgang mit Drittanbieter-Anwendungen			
Remote-Installation von Anwendungen auf Geräten	✓	–	✓ Weitere Informationen finden Sie im folgenden Artikel: Remote-Installation von Anwendungen auf macOS-Geräten.
Programm-Updates	✓	–	–
Anpassen von Updates des Betriebssystems in einer Richtlinie des Administrationsagenten	✓	–	–
Informationen über Schwachstellen in Programmen anzeigen	✓	–	–
Schwachstellensuche in Anwendungen	✓	–	–
Inventarisierung von auf Geräten installierten Programmen	✓	✓	–
Virtuelle Maschinen			
Installation des Administrationsagenten auf einer virtuellen Maschine	✓	✓	✓
Einstellungen für Optimierung der Virtual Desktop Infrastructure (VDI)	✓	✓	✓
Unterstützung von dynamischen virtuellen Maschinen	✓	✓	✓
Anderes			

Funktion des Administrationsagenten	Windows	Linux	macOS
Audit von Aktionen auf einem Remote-Client-Gerät mithilfe der Windows Desktopfreigabe	✓	–	–
Überwachung des Status des Antiviren-Schutzes	✓	✓	✓
Verwaltung von Geräteneustarts	✓	–	–
Unterstützung von Rollbacks des Dateisystems	✓	✓	✓
Verwendung eines Administrationsagenten als Verbindungs-Gateway	✓	✓	✓
Verbindungsmanager	✓	✓	✓
Wechsel des Administrationsagenten von einem Administrationsserver auf einen anderen (automatisch nach Netzwerkstandort)	✓	–	✓
Verbindung des Client-Geräts mit dem Administrationsserver prüfen. "klnagchk"-Tool	✓	✓	✓
Remotedesktopverbindung mit dem Client-Gerät herstellen	✓	–	✓ Unter Verwendung des Virtual Network Computing-Systems (VNC).
Herunterladen eines autonomen Installationspaketes mithilfe des Migrationsassistenten	✓	✓	✓
Zeroconf-Abfrage	–	✓	–
Anzeigen von Informationen über die Hardware von Client-Geräten	✓	✓ Informationen über die Hardware von Linux-Geräten, die von den darauf installierten Administrationsagenten an den Administrationsserver gesendet werden, sind beschränkt auf jene Informationen, die in den Einstellungen des verwalteten Geräts in der Verwaltungskonsole oder Kaspersky Security Center Web Console angegeben sind.	✓ Informationen über die Hardware von macOS-Geräten, die von den darauf installierten Administrationsagenten an den Administrationsserver gesendet werden, sind beschränkt auf jene Informationen, die in den Einstellungen des verwalteten Geräts in der Verwaltungskonsole oder Kaspersky Security Center Web Console angegeben sind.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (im Folgenden auch als Kaspersky Security Center Web Console bezeichnet) ist eine Web-Anwendung, die dafür konzipiert ist, den Sicherheitsstatus von Unternehmensnetzwerken zu kontrollieren, die mit Kaspersky-Anwendungen geschützt werden.

Mithilfe des Programms können Sie folgende Aktionen ausführen:

- Status des Antiviren-Schutzsystems in Ihrem Unternehmen kontrollieren.
- Kaspersky-Anwendungen auf Geräten Ihres Netzwerks installieren und die installierten Anwendungen verwalten.
- Für die Geräte Ihres Netzwerks erstelle Richtlinien verwalten.
- Benutzerkonten verwalten.
- Aufgaben für Anwendungen verwalten, die auf Ihren Netzwerkgeräten installiert sind.
- Berichte über den Schutzstatus anzeigen.
- Versand von Berichten an Systemadministratoren und andere IT-Spezialisten verwalten.

Informationen zu den Hardware- und Softwareanforderungen finden Sie in den Anforderungen der Web Console.

Das Programm Kaspersky Security Center Web Console stellt eine Weboberfläche zur Verfügung, die Ihre Interaktion mit dem Administrationsserver durch den Browser gewährleistet. Beim Administrationsserver handelt es sich um eine Anwendung, das für die Verwaltung der auf Ihren Netzwerkgeräten installierten Kaspersky-Anwendungen konzipiert ist. Der Administrationsserver verbindet sich mit den Geräten Ihres Netzwerks über die geschützten (SSL) Kommunikationskanäle. Wenn Sie mithilfe Ihres Browsers eine Verbindung zur Kaspersky Security Center Web Console herstellen, stellt der Browser eine sichere Verbindung mit dem Server der Web Console von Kaspersky Security Center her.

Kaspersky Security Center Web Console funktioniert auf folgende Weise:

1. Sie stellen eine Verbindung zur Kaspersky Security Center Web Console mithilfe Ihres Browsers her, in dessen Fenster die Seiten des Programm-Webportals angezeigt werden.
2. Mithilfe der Verwaltungselemente des Webportals wählen Sie einen Befehl, den Sie ausführen möchten. Kaspersky Security Center Web Console führt folgende Aktionen aus:
   - Wenn Sie einen Befehl zum Empfangen von Informationen ausgewählt haben (z. B. Geräteliste anzeigen), erstellt Kaspersky Security Center Web Console eine entsprechende Abfrage an den Administrationsserver, empfängt danach die erforderlichen Daten vom Server und leitet sie in einer zur Anzeige geeigneten Ansicht an den Browser weiter.
   - Wenn Sie einen Verwaltungsbefehl ausgewählt haben (z.B. Remote-Installation eines Antiviren-Programms), empfängt Kaspersky Security Center Web Console den Befehl vom Browser und leitet ihn an den Administrationsserver weiter. Danach empfängt das Programm vom Administrationsserver das Ergebnis der Befehlsausführung und leitet es in einer zur Anzeige geeigneten Ansicht an den Browser weiter.

Kaspersky Security Center Web Console ist eine mehrsprachige Anwendung. Sie können die Sprache der Benutzeroberfläche jederzeit und ohne erneutes Öffnen der Anwendung ändern. Wenn Sie Kaspersky Security Center Web Console zusammen mit Kaspersky Security Center installieren, besitzt Kaspersky Security Center Web Console die gleiche Sprache für die Benutzeroberfläche, wie die Installationsdatei. Wenn Sie Kaspersky Security Center Web Console separat installieren, besitzt die Anwendung die gleiche Sprache für die Benutzeroberfläche, wie das Betriebssystem. Wenn Kaspersky Security Center Web Console die Sprache der Installationsdatei oder des Betriebssystems nicht unterstützt, wird standardmäßig Englisch festgelegt.

Die Funktion "Verwaltung mobiler Geräte" wird in der Kaspersky Security Center Web Console nicht unterstützt. Wenn Sie jedoch mobile Geräte mithilfe von Microsoft Management Console zu einer Administrationsgruppe hinzugefügt haben, werden diese Geräte auch in der Kaspersky Security Center Web Console angezeigt.

Diagramm der Bereitstellung für Kaspersky Security Center Administrationsserver und Kaspersky Security Center Web Console

Die nachfolgende Abbildung zeigt das Bereitstellungsdiagramm für Kaspersky Security Center Administrationsserver und Kaspersky Security Center Web Console.

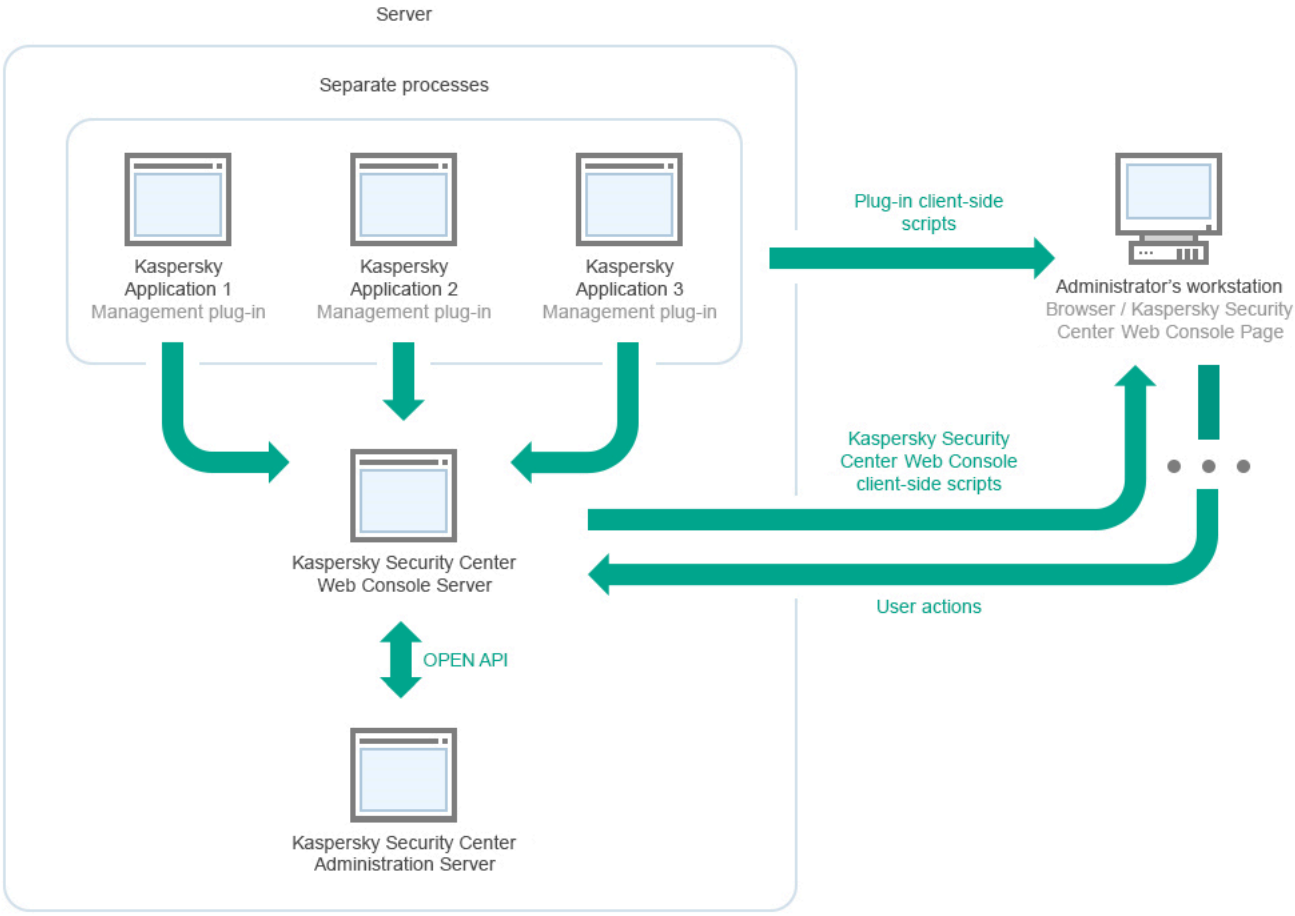


Diagramm der Softwareverteilung für Kaspersky Security Center Administrationsserver und Kaspersky Security Center Web Console

Verwaltungs-Plug-ins für Anwendungen von Kaspersky, die auf geschützten Geräten installiert sind (ein Plug-in für jede Anwendung) werden gemeinsam mit dem Server der Kaspersky Security Center Web Console verteilt.

Als Administrator greifen Sie mittels eines Browsers auf Ihrer Arbeitsstation auf Kaspersky Security Center Web Console zu.

Wenn Sie bestimmte Aktionen in Kaspersky Security Center Web Console durchführen kommuniziert der Server der Web Console von Kaspersky Security Center mit dem Kaspersky Security Center Administrationsserver über OpenAPI. Der Server der Web Console von Kaspersky Security Center fordert die gewünschten Informationen vom Kaspersky Security Center Administrationsserver an und zeigt die Ergebnisse Ihrer Vorgänge in Kaspersky Security Center Web Console an.

Von Kaspersky Security Center Web Console verwendete Ports

Die untenstehende Tabelle listet alle Ports auf, die auf dem Gerät geöffnet werden müssen, auf dem der Server der Web Console von Kaspersky Security Center (auch Kaspersky Security Center Web Console genannt) installiert ist.

Von Kaspersky Security Center Web Console verwendete Ports

Portnummer	Name des Dienstes	Protokoll	Zweck des Ports	Gültigkeitsbereich
2001	Kaspersky Security Center Server für Produkt-Plug-ins	HTTPS	API-Port, der von den Prozessen des Verwaltungs-Plug-ins verwendet wird, um Anfragen vom "Kaspersky Security Center Web Console Management Service" zu empfangen	Ausführen der node.exe-Prozessen der Verwaltungs-Plug-ins
1329, 2003	Verwaltungsdienst der Kaspersky Security Center Web Console	HTTPS	API-Ports, die verwendet werden, um Anfragen vom "Kaspersky Security Center Web Console Management Service" des selben Geräts zu empfangen	Aktualisierung der Komponenten von Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	API-Port, der verwendet wird, um Anfragen vom "Kaspersky Security Center Web Console Management Service" des selben Geräts zu empfangen	Ausführen der node.exe-Prozessen von Kaspersky Security Center Web Console
3333	Kaspersky OSMP KAS-Dienst	HTTPS	Port des OAuth2.0-Autorisierungsendpunkts	Identitäts- und Zugriffsverwaltung (IAM)
4004	Kaspersky OSMP Facade-Dienst	HTTPS	Port des OAuth2.0-Identitätsanbieters	Identitäts- und Zugriffsverwaltung (IAM)
4444	Kaspersky OSMP KAS-Dienst	HTTPS	Port des Introspection-Endpunkts des OAuth2.0 Token	Identitäts- und Zugriffsverwaltung (IAM)
8200	—	HTTP	API-Port, der für die Erstellung von Zertifikaten unter Verwendung von HashiCorp Vault verwendet wird (Weitere Informationen entnehmen Sie der Website von HashiCorp Vault)	Installieren von Kaspersky Security Center Web Console und Aktualisieren der Komponenten von Kaspersky Security Center Web Console
4150, 4151, 4152	Nachrichten-Warteschlange von Kaspersky Security Center Web Console	HTTPS	API-Ports des Message Brokers, die für die Kommunikation zwischen den Prozessen von Kaspersky Security Center Web Console und den Verwaltungs-Plug-ins verwendet werden	Interaktionen zwischen Kaspersky Security Center Web Console und Verwaltungs-Plug-ins

In der folgenden Tabelle sind die Ports aufgeführt, die auf dem Gerät mit dem installierten Server der Web Console von Kaspersky Security Center nicht geöffnet werden müssen. Die Kaspersky Security Center Web Console verwendet diese Ports jedoch für die Identitäts- und Zugriffsverwaltung.

Von Kaspersky Security Center Web Console für Identitäts- und Zugriffsverwaltung verwendete Ports

Portnummer	Name des Dienstes	Protokoll	Zweck des Ports	Gültigkeitsbereich
4445	Kaspersky OSMP KAS-Dienst	HTTPS	Hauptport der Identitäts- und Zugriffsverwaltung, der die Konfiguration von der Kaspersky Security Center Web Console für den Port des OAuth2.0-Autorisierungsendpunkts empfängt (weitere Informationen zu OAuth 2.0 finden Sie auf der Webseite von OAuth)	Identitäts- und Zugriffsverwaltung (IAM)
2444	Kaspersky OSMP Facade-Dienst	HTTPS	Port für die Konfiguration der Identitäts- und Zugriffsverwaltung	Identitäts- und Zugriffsverwaltung (IAM)
2445	Kaspersky OSMP Facade-Dienst	HTTPS	Port für die Verbindung des "Kaspersky OSMP KAS Service" mit dem "Kaspersky OSMP Facade Service"	Identitäts- und Zugriffsverwaltung (IAM)

Benutzeroberfläche der Kaspersky Security Center Web Console

Kaspersky Security Center wird über die Benutzeroberfläche der Kaspersky Security Center Web Console verwaltet.

Das Fenster der Kaspersky Security Center Web Console enthält die folgenden Elemente:

- Hauptmenü im linken Fensterbereich
- Arbeitsbereich im rechten Fensterbereich

Hauptmenü

Das Hauptmenü enthält die folgenden Abschnitte:

- **Administrationsserver**. Zeigt den Namen des Administrationsservers an, mit dem Sie aktuell verbunden sind. Durch Klick auf das Einstellungssymbol ( ) können Sie die Eigenschaften des Administrationsservers öffnen.
- **Überwachung und Berichterstattung**. Bietet einen Überblick über Ihre Infrastruktur, den Schutzstatus und die Statistiken.
- **Assets (Geräte)**. Enthält Werkzeuge für Assets, Aufgaben und Richtlinien der Kaspersky-Anwendungen.
- **Benutzer und Rollen**. Hier können Sie Benutzer und Rollen verwalten, Benutzerrechte durch Rollenzuweisung an Benutzer konfigurieren und Richtlinienprofile mit Rollen verknüpfen.
- **Vorgänge**. Enthält eine Vielzahl von Vorgängen wie die Anwendungslizenzierung, das Anzeigen und Verwalten von verschlüsselten Laufwerken und Verschlüsselungsereignissen sowie die Verwaltung von Drittanbieter-Anwendungen. Dazu gehört auch der Zugriff auf die Datenverwaltungen der Anwendung.
- **Entdeckung und Bereitstellung**. Hier können Sie Netzwerkabfragen durchführen, um Client-Geräte zu finden, und diese Geräte manuell oder automatisch auf Administrationsgruppen verteilen. Dieser Abschnitt enthält außerdem den Schnellstartassistenten und den Assistenten für die Bereitstellung des Schutzes.
- **Marketplace**. Hier finden Sie Informationen über die Unternehmenslösungen von Kaspersky und können passende Lösungen auswählen und anschließend auf der Kaspersky-Website erwerben.

- **Einstellungen**. Hier können Sie ein Backup des aktuellen Zustands eines Web-Plug-ins anlegen und den gespeicherten Zustand später wiederherstellen. Enthält Ihre persönlichen Einstellungen für die Darstellung der Benutzeroberfläche, z. B. die gewählte Sprache für die Benutzeroberfläche oder das Farbschema.

- **Menü Ihres Benutzerkontos**. Enthält einen Link zur Hilfe von Kaspersky Security Center. Sie können sich außerdem von Kaspersky Security Center abmelden und die Version von Kaspersky Security Center Web Console sowie die Liste der installierten Web-Plug-ins zur Verwaltung anzeigen.

Arbeitsbereich

Im Arbeitsbereich werden die Informationen zu den jeweiligen Abschnitten angezeigt, die Sie der Kaspersky Security Center Web Console anwählen. Er enthält außerdem Steuerelemente, mit denen Sie die Darstellung der Informationen anpassen können.

Abschnitte des Hauptmenüs anheften und lösen

Sie können Abschnitte von Kaspersky Security Center Web Console anheften, um sie den Favoriten hinzuzufügen und sie schnell über den Abschnitt **Angepinnt** des Hauptmenüs zu erreichen.

> Wenn keine angehefteten Elemente vorhanden sind, wird der Abschnitt **Angepinnt** nicht im Hauptmenü angezeigt.

Sie können nur Abschnitte anheften, in denen Seiten angezeigt werden. Wenn Sie beispielsweise zum Abschnitt **Assets (Geräte)** → **Verwaltete Geräte** gehen, wird die Seite mit der Gerätetabelle geöffnet. Dies bedeutet, dass Sie den Abschnitt **Verwaltete Geräte** anheften können. Sollte hingegen ein Fenster oder kein Element angezeigt werden, nachdem Sie einen Abschnitt im Hauptmenü ausgewählt haben, können Sie den ausgewählten Abschnitt nicht anheften.

So heften Sie einen Abschnitt an:

1. Bewegen Sie den Mauszeiger im Hauptmenü über den Abschnitt, den Sie anheften möchten.

   Das Pin-Symbol (📌) wird angezeigt.

2. Klicken Sie auf das Pin-Symbol (📌).

Der Abschnitt wird angeheftet und im Abschnitt **Angepinnt** angezeigt.

Sie können Elemente auch aus Ihren Favoriten entfernen, indem Sie diese loslösen.

So lösen Sie einen angehefteten Abschnitt los:

1. Gehen Sie im Hauptmenü zum Abschnitt **Angepinnt**.

2. Bewegen Sie den Mauszeiger über den Abschnitt, den Sie lösen möchten, und klicken Sie anschließend auf das Lösen-Symbol (📌).

Der Abschnitt wird aus den Favoriten entfernt.

Szenario: Installation und Erstkonfiguration von Kaspersky Security Center Web Console

In diesem Szenario wird beschrieben, wie Kaspersky Security Center Administrationsserver und Kaspersky Security Center Web Console installiert werden, der Administrationsserver mithilfe des Schnellstartassistenten initialisiert wird und Kaspersky-Anwendungen auf den verwalteten Geräten mit dem Assistenten für die Bereitstellung des Schutzes installiert werden.

Die Installation und Ersteinrichtung von Kaspersky Security Center Web Console erfolgt in mehreren Schritten:

1. **Installation eines Datenbank-Managementsystems (DBMS)**

   Installation des Datenbank-Managementsystems (DBMS) oder eines anderen Systems, das von Kaspersky Security Center verwendet werden soll.

   Informationen zur Installation des ausgewählten DBMS finden Sie in dessen Dokumentation.

2. **Installation von Administrationsserver, Verwaltungskonsole, Administrationsagent**

   Zusammen mit dem Administrationsserver werden auch die Verwaltungskonsole und die Serverversion des Administrationsagenten installiert.

   Geben Sie während der Konfiguration der Installation von Kaspersky Security Center Administrationsserver an, ob Kaspersky Security Center Web Console auf dem gleichen Gerät installiert werden soll. Wenn Sie beide Komponenten auf demselben Gerät installieren möchten, müssen Sie die Kaspersky Security Center Web Console nicht separat installieren, da sie automatisch installiert wird. Wenn Sie Kaspersky Security Center Web Console auf einem anderen Gerät installieren möchten, gehen Sie nach der Installation von Kaspersky Security Center Administrationsserver zur Installation der Kaspersky Security Center Web Console über.

3. **Kaspersky Security Center Web Console installieren**

   Wenn Sie im vorherigen Schritt nicht die Installation von Kaspersky Security Center Web Console zusammen mit Kaspersky Security Center Administrationsserver ausgewählt haben, installieren Sie Kaspersky Security Center Web Console separat. Sie können Kaspersky Security Center Web Console auf einem anderen Gerät oder auf demselben Gerät installieren, auf dem der Administrationsserver installiert ist.

4. **Erstkonfiguration vornehmen**

   Nach Abschluss der Installation des Administrationsservers wird bei der ersten Verbindung mit dem Administrationsserver automatisch der Schnellstartassistent ausgeführt. Befolgen Sie die Schritte des Assistenten, um die Erstkonfiguration des Administrationsservers nach Bedarf vorzunehmen. Während der Erstkonfiguration erstellt der Assistent die zur Bereitstellung des Schutzes notwendigen Richtlinien und Aufgaben mit Standardeinstellungen. Diese Einstellungen sind eventuell nicht optimal für Ihr Unternehmen geeignet. Sie können bei Bedarf die Einstellungen der Richtlinien und Aufgaben ändern.

5. **Lizenzierung von Kaspersky Security Center (optional)**

   Kaspersky Security Center unterstützt die Basisfunktionen der Verwaltungskonsole, ohne eine Lizenz zu benötigen. Sie benötigen eine kommerzielle Lizenz, wenn Sie eine oder mehrere der zusätzlichen Funktionen verwenden möchten, darunter "Schwachstellen- und Patch-Management", "Verwaltung mobiler Geräte" und "Integration mit SIEM-Systemen". Eine Schlüsseldatei oder einen Aktivierungscode für diese Funktionen können Sie beim entsprechenden Schritt des Schnellstartassistenten oder manuell hinzufügen.

6. **Suche der Geräte im Netzwerk**

   Diese Etappe ist Teil des Schnellstartassistenten. Sie können die Geräte auch manuell finden. Daraufhin erhält Kaspersky Security Center die Adressen und die Namen aller Geräte, die im Netzwerk registriert sind. Im Folgenden können Sie mithilfe von Kaspersky Security Center die Anwendungen von Kaspersky und von anderen Herstellern auf den gefundenen Geräten installieren. Da Kaspersky Security Center die Gerätesuche regelmäßig startet, werden neue Geräte im Netzwerk automatisch gefunden, sobald sie auftauchen.

7. **Geräte in Administrationsgruppen anordnen**

   Diese Etappe ist Teil des Schnellstartassistenten, aber Sie können die gefundenen Geräte auch manuell in Gruppen verschieben.

8. **Installation des Administrationsagenten und der Sicherheitsanwendungen auf den Geräten im Netzwerk**

   Als Bereitstellung des Schutzes im Unternehmensnetzwerk wird die Installation des Administrationsagenten sowie einer Sicherheitsanwendung (z. B. Kaspersky Endpoint Security für Windows) auf den Geräten verstanden, die vom Administrationsserver bei der Gerätesuche im Unternehmensnetzwerk gefunden wurden.

   Um die Anwendungen remote zu installieren, führen Sie den Assistenten für die Bereitstellung des Schutzes aus.

   Die Sicherheitsanwendungen schützen Geräte vor Viren und anderen Anwendungen, die eine Bedrohung darstellen. Der Administrationsagent gewährleistet die Verbindung des Geräts mit dem Administrationsserver. Die Einstellungen des Administrationsagenten werden standardmäßig automatisch angepasst.

   Bevor Sie den Administrationsagenten und die Sicherheitsanwendung auf Geräten im Netzwerk installieren, stellen Sie sicher, dass diese Geräte verfügbar (aktiviert) sind.

9. **Lizenzschlüssel auf Client-Geräte verteilen**

   Verteilen Sie die Lizenzschlüssel auf die Client-Geräte, um die verwalteten Sicherheitsanwendungen auf diesen Geräten zu aktivieren.

10. **Installieren von Kaspersky Security für mobile Endgeräte (optional)**

    Wenn Sie mobile Unternehmensgeräte verwalten möchten, folgen Sie den Anweisungen in der Hilfe von Kaspersky Security für mobile Endgeräte, um Informationen zur Bereitstellung von Kaspersky Endpoint Security für Android zu erhalten.

11. **Konfigurieren von Richtlinien für Kaspersky-Anwendungen**

    Um verschiedene Anwendungseinstellungen auf verschiedene Geräte anzuwenden, können Sie eine geräteorientierte Sicherheitsverwaltung und/oder eine Benutzerorientierte Sicherheitsverwaltung verwenden. Die geräteorientierte Sicherheitsverwaltung kann über Richtlinien und Aufgaben implementiert werden. Sie können Aufgaben nur auf die Geräte anwenden, die bestimmte Bedingungen erfüllen. Um Bedingungen für das Filtern von Geräten festzulegen, verwenden Sie die Geräteauswahl und Tags.

12. **Überwachen des Netzwerkschutzstatus**

    Sie können Ihr Netzwerk mithilfe von Widgets auf dem Dashboard überwachen, Berichte in Kaspersky-Anwendungen erstellen sowie von Anwendungen auf verwalteten Geräten empfangene Ereignisauswahlen und Benachrichtigungslisten anzeigen.

Installation

Dieser Abschnitt beschreibt die Installation für Kaspersky Security Center und Kaspersky Security Center Web Console.

Kaspersky Security Center installieren (Standardinstallation)

In diesem Ablauf wird beschrieben, wie Kaspersky Security Center installiert wird. Vor der Installation müssen Sie ein Datenbankverwaltungssystem installieren.

Um Kaspersky Security Center zu installieren, gehen Sie wie folgt vor:

1. Führen Sie unter einem Benutzerkonto mit Administratorrechten die Datei ksc_<Build-Nummer>_full_<Sprachversion>.exe aus.
2. Klicken Sie im folgenden Fenster zur Auswahl der Anwendung auf **Kaspersky Security Center installieren**.

   Der Installationsassistent für den Kaspersky Security Center Administrationsserver wird gestartet.
3. Beginnen Sie auf der Begrüßungsseite und durchlaufen Sie den Assistenten mit der Schaltfläche **Weiter**.
4. Wenn das Microsoft .NET Framework nicht installiert ist, installieren Sie es.
5. Akzeptieren Sie die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie.
6. Wählen Sie den Installationstyp aus. Zu Testzwecken wird es empfohlen, die voreingestellte Option **Standard** beizubehalten.
7. Wenn Sie Kaspersky Security Center Web Console auf demselben Gerät installieren möchten, aktivieren Sie das Kontrollkästchen **Kaspersky Security Center Web Console installieren**.

   Wenn Sie das Kontrollkästchen deaktivieren, können Sie Kaspersky Security Center Web Console später separat auf demselben oder einem anderen Gerät installieren.
8. Wählen Sie die Größe Ihres Netzwerks aus. Zu Testzwecken wird es empfohlen, die voreingestellte Option **Bis 100 Geräte im Netzwerk** beizubehalten.
9. Wählen Sie den Typ des zuvor installierten Datenbankservers aus.
10. Geben Sie die Verbindungsparameter für den zuvor installierten Datenbankserver an.
11. Geben Sie die Authentifizierungsparameter für den zuvor installierten Datenbankserver an.
12. Klicken Sie auf die Schaltfläche **Installieren**, um die Installation zu beginnen.
13. Geben Sie nach erfolgreichem Abschluss der Installation an, ob die Verwaltungskonsole direkt nach dem Abschluss des Assistenten gestartet werden soll.

    Wenn Sie das Öffnen der Kaspersky Security Center Web Console gewählt haben, wird der Anmeldebildschirm geöffnet. Anschließend können Sie die Erstkonfiguration des Administrationsservers mithilfe des Schnellstartassistenten vornehmen.

    Sie können die Kaspersky Security Center Web Console nur öffnen, wenn sie bereits installiert ist. Sie können die Kaspersky Security Center Web Console nicht öffnen, wenn Sie diese weder während der Installation von Kaspersky Security Center noch separat installiert haben.

14. Klicken Sie im folgenden Fenster der Verwaltungskonsole auf den installierten Administrationsserver.

15. Klicken Sie im folgenden Fenster mit dem Zertifikat des Administrationsservers auf die Schaltfläche **Ja**, um fortzufahren.

Der Schnellstartassistent des Administrationsservers wird gestartet, wenn Sie ihn nicht über web-basierte Verwaltungskonsole ausgeführt haben.

Problemlösung

Wenn das Fenster mit dem Zertifikat des Administrationsservers nicht geöffnet wird und Verbindungsfehler angezeigt werden, versuchen Sie Folgendes:

1. Öffnen Sie in Windows die **Dienste** (**Systemsteuerung** → **Verwaltung** → **Dienste**). Überprüfen Sie, ob die Dienste "Kaspersky Security Center Network Agent" und "Kaspersky Security Center Administration Server" ausgeführt werden.

2. Öffnen Sie in Windows die **Ereignisanzeige** (**Systemsteuerung** → **Verwaltung** → **Ereignisanzeige**) und wählen Sie anschließend **Anwendungs- und Dienstprotokolle** → **Kaspersky-Ereignisprotokoll** aus. Stellen Sie sicher, dass das im Protokoll keine Fehler enthält und Ereignisse wie **Administrationsserver <Versionsnummer> wird ausgeführt** darin vorkommen.

Kaspersky Security Center Web Console installieren

In diesem Abschnitt wird beschrieben, wie Sie den Server der Web Console von Kaspersky Security Center (auch als Kaspersky Security Center Web Console bezeichnet) separat installieren. Vor der Installation müssen Sie ein DBMS und den Kaspersky Security Center Administrationsserver installieren. Sie können Kaspersky Security Center Web Console entweder auf demselben Gerät installieren, auf dem Kaspersky Security Center installiert ist, oder auf einem anderen Gerät.

So installieren Sie Kaspersky Security Center Web Console:

1. Führen Sie unter einem Benutzerkonto mit Administratorrechten die ausführbare Datei ksc-web-console-<Versionsnummer>.<Buildnummer>.exe aus.

   Der Installationsassistent wird gestartet.

2. Wählen Sie die Sprache des Installationsassistenten.

3. Klicken Sie im Willkommensfenster auf **Weiter**.

4. Lesen Sie im Fenster **Lizenzvertrag** die Bedingungen des Endbenutzer-Lizenzvertrags durch und akzeptieren Sie diese. Sobald Sie die EULA akzeptieren, wird die Installation fortgesetzt. Andernfalls ist die Schaltfläche **Weiter** nicht verfügbar.

5. Wählen Sie im Fenster **Zielordner** einen Ordner, in dem Kaspersky Security Center Web Console installiert werden soll (standardmäßig %Programme%\Kaspersky Lab\Kaspersky Security Center Web Console). Wenn dieser Ordner nicht vorhanden ist, wird er automatisch bei der Installation angelegt.

   Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** ändern.

6. Geben Sie im Fenster **Verbindungseinstellungen für Kaspersky Security Center Web Console** die folgenden Informationen an:

   - Adresse der Kaspersky Security Center Web Console (standardmäßig 127.0.0.1).
   - Port, den Kaspersky Security Center Web Console für eingehende Verbindungen verwendet, d. h. der Port, der Zugang zu Kaspersky Security Center Web Console über einen Browser ermöglicht (standardmäßig 8080).

   Es wird empfohlen, die Standardwerte für Adresse und Port beizubehalten.

   Bei Bedarf können Sie auf **Überprüfen** klicken, um sicherzustellen, dass der gewählte Port verfügbar ist.

   Wenn Sie die Protokollierung der Aktivitäten der Kaspersky Security Center Web Console aktivieren möchten, wählen Sie die entsprechende Option. Wenn Sie diese Option nicht aktivieren, werden von Kaspersky Security Center Web Console keine Logdateien angelegt.

7. Geben Sie im Fenster **Benutzerkonto-Einstellungen** die Namen und Kennwörter der Benutzerkonten an.

   Wir empfehlen, Standardkonten zu verwenden.

8. Wählen Sie im Fenster **Client-Zertifikat** eins der Folgenden aus:

   - **Neues Zertifikat erstellen**. Diese Option wird empfohlen, wenn Sie kein Browser-Zertifikat haben.
   - **Existierendes Zertifikat auswählen**. Wählen Sie diese Option, wenn Sie bereits ein Browser-Zertifikat haben. Geben Sie in diesem Fall den Pfad dazu an.
   - Wenn Sie sich entschieden haben, ein neues Zertifikat zu generieren, informiert Sie der Browser beim Öffnen der Kaspersky Security Center Web Console möglicherweise darüber, dass die Verbindung zur Kaspersky Security Center Web Console nicht privat und das Zertifikat der Kaspersky Security Center Web Console ungültig ist. Diese Warnung wird angezeigt, weil das Zertifikat der Kaspersky Security Center Web Console selbstsigniert ist und von Kaspersky Security Center automatisch generiert wird. Um diese Warnung zu vermeiden, erstellen Sie ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt. Wählen Sie als nächstes die Option **Existierendes Zertifikat auswählen** im Fenster **Client-Zertifikat** und geben Sie anschließend den Pfad zu Ihrem benutzerdefinierten Zertifikat an.

   Zertifikate im pfx-Format werden von Kaspersky Security Center Web Console nicht unterstützt. Um ein solches Zertifikat zu verwenden, müssen Sie dieses zunächst mithilfe eines OpenSSL-basierten Cross-Plattform-Tools, wie "OpenSSL for Windows", in das unterstützte pem-Format konvertieren.

9. Stellen Sie im Fenster **Vertrauenswürdige Administrationsserver** sicher, dass die Liste Ihren Administrationsserver enthält, und klicken Sie auf **Weiter**, um zum letzten Fenster des Installers zu wechseln.

   Wenn Sie der Liste einen neuen Administrationsserver hinzufügen möchten, klicken Sie auf die Schaltfläche **Hinzufügen**. Geben Sie im geöffneten Fenster die Eigenschaften für einen neuen vertrauenswürdigen Administrationsservers an:

   - **Name des Administrationsservers**

     Der Name des Administrationsservers, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt wird.

   - **Adresse des Administrationsservers**

     Die IP-Adresse des Geräts, auf dem Sie den Administrationsserver installieren.

- **Port des Administrationsservers**

  Der OpenAPI-Port, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).

- **Zertifikat des Administrationsservers**

  Die Zertifikatsdatei wird auf dem Gerät gespeichert, auf dem der Administrationsserver installiert ist. Der Standardpfad zum Zertifikat des Administrationsservers ist:

  - Für Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
  - Für Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/

  Wenn Sie die Kaspersky Security Center Web Console auf demselben Gerät installieren, auf dem auch der Administrationsserver installiert ist, verwenden Sie einen der oben angegebenen Pfade. Andernfalls kopieren Sie die Zertifikatsdatei vom Gerät mit installiertem Administrationsserver auf das Gerät, auf dem Sie Kaspersky Security Center Web Console installieren, und geben Sie anschließend den lokalen Pfad zum Zertifikat an.

10. Geben Sie im Fenster **Identitäts- und Zugriffsverwaltung (IAM)** an, ob Sie die Identitäts- und Zugriffsverwaltung (auch als IAM bezeichnet) installieren möchten. Wenn Sie die Identitäts- und Zugriffsverwaltung installieren möchten, geben Sie die folgenden Portnummern an:

    - **KAS-Administratorport**. Standardmäßig wird Port 4445 verwendet, um die Konfiguration der Kaspersky Security Center Web Console für den Port des OAuth2.0-Autorisierungsendpunkts zu empfangen.
    - **Facade-Administratorport**. Standardmäßig wird Port 2444 für die Konfiguration der Identitäts- und Zugriffsverwaltung verwendet.
    - **Facade-Interaktionsport**. Standardmäßig wird Port 2445 für die Verbindung des Kaspersky OSMP KAS-Dienstes mit dem Kaspersky OSMP Facade-Dienst verwendet.

    Bei Bedarf können Sie die standardmäßigen Portnummern ändern. Später können diese nicht mehr über die Kaspersky Security Center Web Console geändert werden.

11. Klicken Sie im letzten Fenster des Installers auf **Installieren**, um mit der Installation zu beginnen.

Nach dem erfolgreichen Abschluss der Installation wird auf Ihrem Desktop eine Verknüpfung angezeigt und Sie können sich in der Kaspersky Security Center Web Console einloggen.

Der Schnellstartassistent für den Administrationsserver wird gestartet, falls Sie ihn nicht über die auf der Microsoft Management Console basierenden Verwaltungskonsole geöffnet haben.

Problemlösung

Wenn Kaspersky Security Center Web Console unter der von Ihnen eingegebenen URL nicht in Ihrem Browser angezeigt wird, versuchen Sie Folgendes:

1. Überprüfen Sie, ob Sie den korrekten Hostnamen bzw. die korrekte IP-Adresse des Geräts eingegeben haben, auf dem Kaspersky Security Center Web Console installiert ist.
2. Überprüfen Sie, ob das Gerät, mit dem Sie arbeiten möchten, Zugriff auf das Gerät hat, auf dem Kaspersky Security Center Web Console installiert ist.
3. Überprüfen Sie, ob die Einstellungen der Firewall auf dem Gerät, auf dem Kaspersky Security Center Web Console installiert ist, eingehende Verbindungen über Port 8080 und für die Anwendung node.exe erlauben.

4. Öffnen Sie in Windows die **Dienste**. Überprüfen Sie, ob der Dienst für Kaspersky Security Center Web Console ausgeführt wird.

5. Überprüfen Sie, ob Sie mithilfe der Verwaltungskonsole auf Kaspersky Security Center zugreifen können.

6. Öffnen Sie in Windows die **Ereignisanzeige** und wählen Sie dann **Anwendungs- und Dienstprotokolle → Kaspersky-Ereignisprotokoll** aus. Vergewissern Sie sich, dass das Protokoll keine Fehler enthält.

Installation der Kaspersky Security Center Web Console mit Verbindung zum Administrationsserver, der auf Knoten des Failover-Clusters installiert wurde

In diesem Abschnitt wird die Installation des Servers der Web Console von Kaspersky Security Center (im Folgenden auch als "Kaspersky Security Center Web Console" bezeichnet) beschrieben, der eine Verbindung zu dem auf den Knoten eines Kaspersky Security Center Failover-Clusters oder Windows Server Failover-Clusters installierten Administrationsserver herstellt. Installieren Sie vor der Installation von Kaspersky Security Center Web Console ein DBMS und den Kaspersky Security Center Administrationsserver auf den Knoten des Kaspersky Security Center Failover-Clusters oder den Knoten des Windows Server Failover-Clusters.

> Wenn Sie einen Windows Server-Failover-Cluster verwenden, empfehlen wir, Kaspersky Security Center Web Console nicht auf einem Failover-Cluster-Knoten zu installieren. Im Falle eines Ausfalls des Knotens verlieren Sie den Zugriff auf den Administrationsserver.

So installieren Sie die Kaspersky Security Center Web Console, die eine Verbindung zu dem auf den Knoten des Kaspersky-Failover-Clusters installierten Administrationsserver herstellt:

1. Folgen Sie den Schritten des Abschnitts Kaspersky Security Center Web Console installieren von Schritt 1 bis Schritt 8.

2. In Schritt 9: Klicken Sie in dem Fenster **Vertrauenswürdige Administrationsserver** auf die Schaltfläche **Hinzufügen**, um ein Failover-Cluster als vertrauenswürdigen Administrationsserver hinzuzufügen.

   Geben Sie im geöffneten Fenster die folgenden Eigenschaften an:

   - **Name des Administrationsservers**

     Der Name des Clusters, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt wird.

   - **Adresse des Administrationsservers**

     Geben Sie die Clusteradresse je nach Art des Failover-Clusters an:

     - **Kaspersky Security Center Failover-Cluster**. Geben Sie die IP-Adresse des sekundären Netzwerkadapters als Adresse des Clusters an, wenn Sie den Adapter beim Vorbereiten der Cluster-Knoten erstellt haben. Geben Sie andernfalls die IP-Adresse eines von Ihnen verwendeten Load Balancers eines Drittanbieters an.

     - **Windows Server-Failover-Cluster**. Geben Sie die Cluster-Adresse an, die Sie beim Erstellen des Windows Server Failover-Clusters erhalten haben.

   - **Port des Administrationsservers**

     Der OpenAPI-Port, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).

- **Zertifikat des Administrationsservers**

  Das Zertifikat des Administrationsservers befindet sich im freigegebenen Datenspeicher des Kaspersky Security Center Failover-Clusters oder des Windows Server Failover-Clusters. Der Standardpfad zur Zertifikatsdatei lautet: <freigegebener Datenordner>\1093\cert\klserver.cer. Kopieren Sie die Zertifikatsdatei aus dem freigegebenen Datenspeicher auf das Gerät, auf dem Sie Kaspersky Security Center Web Console installieren. Geben Sie den lokalen Pfad zum Zertifikat des Administrationsservers an.

3. Fahren Sie mit der standardmäßigen Installation von Kaspersky Security Center Web Console fort.

Nach dem Abschluss der Installation wird auf Ihrem Desktop eine Verknüpfung angezeigt und Sie können sich in der Kaspersky Security Center Web Console anmelden.

Aktualisieren von Kaspersky Security Center Web Console

Wenn Sie aktuellere Versionen von Kaspersky Security Center Web Console verwenden wollen, ohne dabei Ihre aktuell installierte Instanz zu entfernen, können Sie den Standardvorgang zum Aktualisieren aus dem Installer von Kaspersky Security Center Web Console verwenden.

Um Kaspersky Security Center Web Console zu aktualisieren:

1. Führen Sie unter einem Benutzerkonto mit Administratorrechten die ausführbare Installationsdatei ksc-web-console-<Versionsnummer>.<Build-Nummer>.exe aus, wobei "<Build-Nummer>" für einen Build von Kaspersky Security Center Web Console steht, dessen Build-Nummer höher ist, als die Ihrer aktuell installierten Instanz.

2. Wählen Sie in dem sich öffnenden Fenster des Installationsassistenten die Sprache aus und klicken Sie auf **OK**.

3. Wählen Sie im Begrüßungsfenster die Option **Upgrade** aus und klicken Sie auf **Weiter**.

4. Lesen Sie im Fenster **Lizenzvertrag** die Bedingungen des Endbenutzer-Lizenzvertrags durch und akzeptieren Sie diese. Sobald Sie die EULA akzeptieren, wird die Installation fortgesetzt. Andernfalls ist die Schaltfläche **Weiter** nicht verfügbar.

5. Fahren Sie mit dem Installationsassistenten fort, bis die Installation abgeschlossen ist. Während des Fortsetzens können Sie ebenfalls die Einstellungen von Kaspersky Security Center Web Console, die Sie während einer früheren Installation angegeben haben, anpassen. Klicken Sie im Schritt **Bereit zur Änderung von Kaspersky Security Center Web Console** auf die Schaltfläche **Upgrade**. Warten Sie, bis die neuen Einstellungen übernommen wurden, und klicken Sie im nächsten Schritt des Installationsassistenten auf **Fertigstellen**. Alternativ können Sie auf den Link **Kaspersky Security Center Web Console in Ihrem Browser starten** klicken, um die aktualisierte Instanz von Kaspersky Security Center Web Console sofort zu starten.

   > Das Anpassen der Einstellungen von Kaspersky Security Center Web Console während der Aktualisierung ist nur für Kaspersky Security Center Web Console ab Version 12.2 verfügbar.

   Ihre Instanz der Kaspersky Security Center Web Console wurde aktualisiert.

Zertifikate für die Ausführung mit Kaspersky Security Center Web Console

In diesem Abschnitt wird beschrieben, wie Sie Zertifikate für Kaspersky Security Center Web Console ausstellen und ersetzen und wie Sie ein Zertifikat für den Administrationsserver erneuern, wenn der Server mit Kaspersky Security Center Web Console interagiert.

Zertifikat für Kaspersky Security Center Web Console erneut ausstellen

In den meisten Browser gilt eine maximale Gültigkeitsdauer für Zertifikate. Um diese Bedingung einzuhalten, ist die Gültigkeitsdauer des Zertifikats für Kaspersky Security Center Web Console auf 397 Tage begrenzt. Sie können ein existierendes Zertifikat, dass Sie von einer Zertifizierungsstelle (Certification Authority, CA) erhalten haben, durch das Ausstellen eines neuen, selbstsignierten Zertifikats ersetzen. Alternativ können Sie Ihr abgelaufenes Zertifikat von Kaspersky Security Center Web Console neu ausstellen.

Das Zertifikat für Kaspersky Security Center Web Console kann nicht automatisch neu ausgestellt werden. Sie müssen das abgelaufene Zertifikat manuell neu ausstellen.

Wenn Sie bereits ein selbstsigniertes Zertifikat verwenden, können Sie dieses ebenfalls erneut ausstellen, indem Sie Kaspersky Security Center Web Console mittels Standardverfahren des Installers (Option **Upgrade**) aktualisieren.

Wenn Sie die Web Console öffnen, informiert Sie der Browser möglicherweise darüber, dass die Verbindung zur Web Console nicht privat und das Zertifikat der Web Console ungültig ist. Diese Warnung wird angezeigt, weil das Zertifikat der Web Console selbstsigniert ist und von Kaspersky Security Center automatisch generiert wird. Um diese Warnung zu entfernen oder zu vermeiden, können Sie Folgendes tun:

- Geben Sie bei der Neuausstellung des Zertifikats ein benutzerdefiniertes Zertifikat an (empfohlene Option). Erstellen Sie ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt.

- Fügen Sie das Zertifikat der Web Console nach der Neuausstellung der Liste mit vertrauenswürdigen Browser-Zertifikaten hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können.

Um bei der ersten Installation von Kaspersky Security Center Web Console ein neues Zertifikate auszustellen:

1. Starten Sie die Standardinstallation von Kaspersky Security Center Web Console.

2. Wählen Sie im Schritt **Client-Zertifikat** des Installationsassistenten die Option **Neues Zertifikat erstellen** aus, und klicken Sie anschließend auf **Weiter**.

3. Fahren Sie mit den verbleibenden Schritten des Installationsassistenten fort, bis die Installation abgeschlossen ist.

   Für Kaspersky Security Center Web Console wurde ein neues Zertifikat mit einem Gültigkeitszeitraum von 397 Tagen ausgestellt.

Um ein abgelaufenes Zertifikat von Kaspersky Security Center Web Console erneut auszustellen:

1. Führen Sie unter einem Benutzerkonto mit Administratorrechten die Installationsdatei ksc-web-console-<Versionsnummer>.<Buildnummer>.exe aus.

2. Wählen Sie in dem sich öffnenden Fenster des Installationsassistenten die Sprache aus und klicken Sie auf **OK**.

3. Wählen Sie im Begrüßungsfenster die Option **Zertifikat erneut ausstellen** aus und klicken Sie auf **Weiter**.

4. Warten Sie im nächsten Schritt ab, bis die Neukonfiguration von Kaspersky Security Center Web Console abgeschlossen wurde, und klicken Sie auf **Fertigstellen**.

   Das Zertifikat von Kaspersky Security Center Web Console wurde erneut für einen weiteren Gültigkeitszeitraum von 397 Tagen ausgestellt.

Wenn Sie die Identitäts- und Zugriffsverwaltung verwenden, müssen Sie auch alle TLS-Zertifikate für die Ports, die von der Identitäts- und Zugriffsverwaltung verwendet werden, neu ausstellen. Wenn ein Zertifikat abläuft, zeigt die Kaspersky Security Center Web Console eine Benachrichtigung an. Sie müssen die Anweisungen der Benachrichtigung befolgen.

Zertifikat für Kaspersky Security Center Web Console ersetzen

Wenn Sie den Server der Web Console von Kaspersky Security Center installieren, wird standardmäßig automatisch ein Browser-Zertifikat für das Programm generiert. Sie können das automatisch generierte Zertifikat mit einem eigenen ersetzen.

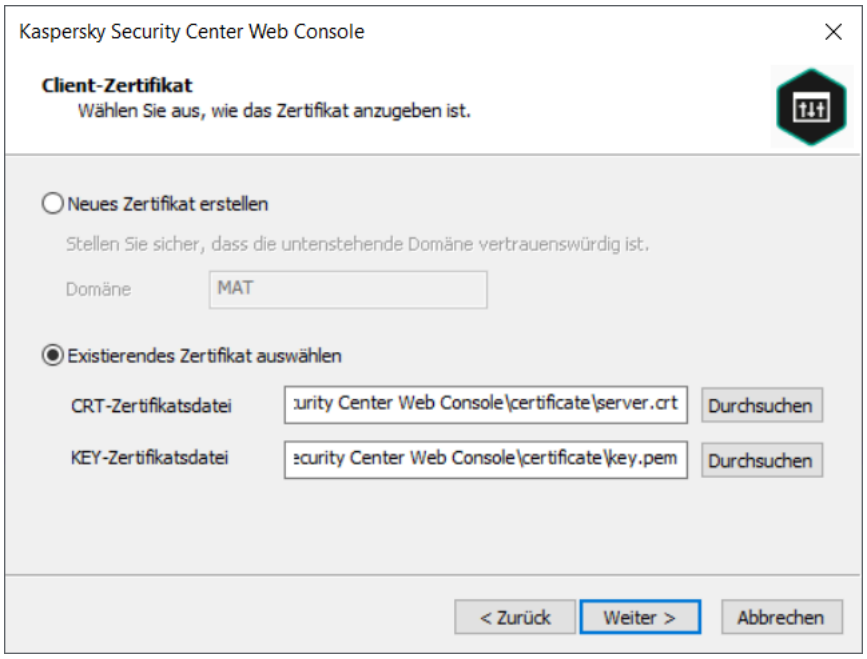
Um das Zertifikat für den Server der Web Console von Kaspersky Security Center mit einem eigenen zu ersetzen, gehen Sie wie folgt vor:

1. Führen Sie auf dem Gerät, auf dem der Server der Web Console von Kaspersky Security Center installiert ist, die ausführbare Datei ksc-web-console.<Versionsnummer>.<Build-Nummer>.exe unter einem Benutzerkonto mit Administratorrechten aus.

   Der Installationsassistent wird gestartet.

2. Wählen Sie auf der ersten Seite des Assistenten die Option **Upgrade** aus.

3. Wählen Sie auf der Seite **Client-Zertifikat** die Option **Wählen Sie ein existierendes Zertifikat** aus und geben Sie den Pfad zum benutzerdefinierten Zertifikat an.



Angeben des Client-Zertifikats

4. Klicken Sie auf der letzten Seite des Assistenten auf **Ändern**, um die neuen Einstellungen zu übernehmen.

5. Nach dem erfolgreichen Abschluss der Neukonfigurierung des Programms klicken Sie auf die Schaltfläche **Fertigstellen**.

Die Kaspersky Security Center Web Console verwendet jetzt das angegebene Zertifikat.

Zertifikaten für vertrauenswürdige Administrationsserver in der Kaspersky Security Center Web Console angeben

Das vorhandene Zertifikat des Administrationsservers wird vor dem Ablaufdatum des Zertifikats automatisch mit einem neuen Zertifikat ersetzt. Das vorhandene Zertifikat des Administrationsservers kann auch durch ein benutzerdefiniertes Zertifikat ersetzt werden. Bei jeder Änderung des Zertifikats muss das neue Zertifikat in den Einstellungen der Kaspersky Security Center Web Console angegeben werden. Andernfalls kann die Kaspersky Security Center Web Console keine Verbindung zum Administrationsserver herstellen.

Um ein neues Zertifikat für den Administrationsserver anzugeben, gehen Sie wie folgt vor:

1. Kopieren Sie auf dem Gerät, auf dem der Administrationsserver installiert ist, die Zertifikatsdatei auf ein Massenspeichergerät oder Ähnliches.

   Standardmäßig wird die Zertifikatsdatei im folgenden Ordner gespeichert:

   - Für Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Für Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/

2. Platzieren Sie auf dem Gerät, auf dem die Kaspersky Security Center Web Console installiert ist, die Zertifikatsdatei in einem lokalen Ordner.

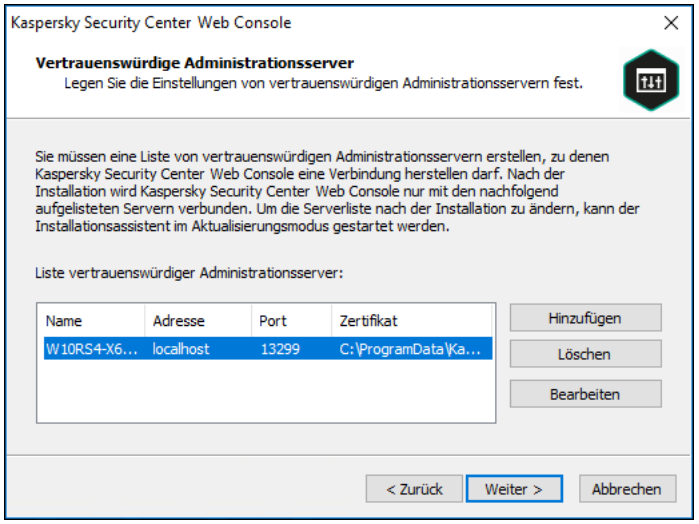
3. Führen Sie die Installationsdatei ksc-web-console-<Versionsnummer>.<Build-Nummer>.exe unter einem Benutzerkonto mit Administratorrechten aus.

   Der Installationsassistent wird gestartet.

4. Wählen Sie auf der ersten Seite des Assistenten die Option **Upgrade**.

   Folgen Sie den Anweisungen des Assistenten.

5. Wählen Sie auf der Seite **Vertrauenswürdige Administrationsserver** den gewünschten den gewünschten Administrationsserver aus und klicken Sie auf die Schaltfläche **Bearbeiten**.



Angabe der vertrauenswürdigen Administrationsserver

6. Klicken Sie in dem geöffneten Fenster **Administrationsserver bearbeiten** auf die Schaltfläche **Durchsuchen**, geben Sie den Pfad zur neuen Zertifikatsdatei an und klicken Sie auf die Schaltfläche **Update** um die Änderungen anzuwenden.

7. Klicken Sie auf der Seite **Bereit zur Änderung von Kaspersky Security Center Web Console** des Assistenten auf die Schaltfläche **Upgrade**, um das Upgrade zu starten.

8. Nach dem erfolgreichen Abschluss der Neukonfigurierung des Programms klicken Sie auf die Schaltfläche **Fertigstellen**.

9. Melden Sie sich an der Kaspersky Security Center Web Console an.

Die Kaspersky Security Center Web Console verwendet jetzt das angegebene Zertifikat.

Konvertieren eines pfx-Zertifikats in ein pem-Zertifikat

Um in Kaspersky Security Center Web Console ein pfx-Zertifikat zu verwenden, müssen Sie dieses zunächst unter Verwendung eines beliebigen OpenSSL-basierten Cross-Plattform-Tools in ein pem-Format konvertieren.

So konvertieren unter Windows ein pfx-Zertifikat in ein pem-Zertifikat:

1. Führen Sie in einem OpenSSL-basierten Cross-Plattform-Tool die folgenden Befehle aus:

   ```
   openssl pkcs12 -in <Dateiname.pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in <Dateiname.pfx> -nocerts -nodes -out key.pem
   ```

   Daraufhin erhalten Sie einen öffentlichen Schlüssel in Form einer crt-Datei und einen privaten Schlüssel als kennwortgeschützte pem-Datei.

2. Stellen Sie sicher, dass die crt-Datei und die pem-Datei in dem gleichen Ordner generiert werden, in dem sich die pfx-Datei befindet.

3. Wenn die crt-Datei oder die pem-Datei sog. "Bag Attributes" enthalten, löschen Sie diese Attribute mit einem Texteditor Ihrer Wahl und speichern Sie die Dateien.

4. Starten Sie den Windows-Dienst neu.

5. Kaspersky Security Center Web Console unterstützt keine kennwortgeschützten Zertifikate. Führen Sie daher in einem OpenSSL-basierten, plattformübergreifenden Tool den folgenden Befehl aus, um das Kennwort von der pem-Datei zu entfernen:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Verwenden Sie für die Input- und Output-Dateien nicht denselben Namen.

   Daraufhin ist die neue pem-Datei nicht mehr kennwortgeschützt. Um sie zu verwenden, muss kein Kennwort mehr eingegeben werden.

Die crt- und die pem-Datei sind bereit zur Verwendung. Sie können diese im Installer von Kaspersky Security Center Web Console angeben.

So konvertieren Sie unter Linux ein pfx-Zertifikat in ein pem-Format:

1. Führen Sie in einem OpenSSL-basierten Cross-Plattform-Tool die folgenden Befehle aus:

   ```
   openssl pkcs12 -in <Dateiname.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <Dateiname.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Stellen Sie sicher, dass die Zertifikatsdatei und der private Schlüssel in dem gleichen Verzeichnis generiert werden, in dem sich die pfx-Datei befindet.

3. Kaspersky Security Center Web Console unterstützt keine kennwortgeschützten Zertifikate. Führen Sie daher in einem OpenSSL-basierten, plattformübergreifenden Tool den folgenden Befehl aus, um das Kennwort von der pem-Datei zu entfernen:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Verwenden Sie für die Input- und Output-Dateien nicht denselben Namen.

   Daraufhin ist die neue pem-Datei nicht mehr kennwortgeschützt. Um sie zu verwenden, muss kein Kennwort mehr eingegeben werden.

Die crt- und die pem-Datei sind bereit zur Verwendung. Sie können diese im Installer von Kaspersky Security Center Web Console angeben.

Migration von Kaspersky Security Center Windows

Dieser Abschnitt beschreibt die Migration verwalteter Geräte und zugehöriger Objekte (Richtlinien, Aufgaben, Gruppen, Tags und andere Objekte) von Kaspersky Security Center Windows zu:

- Kaspersky Security Center Cloud Console
- Kaspersky Security Center Linux

Migration nach Kaspersky Security Center Cloud Console

Sie können die Migration von Kaspersky Security Center Web Console nach Kaspersky Security Center Cloud Console durchführen. Anschließend erhalten Sie Zugriff auf den Administrationsserver und das Datenbankverwaltungssystem (DBMS), die beide in der Kaspersky-Infrastruktur gehostet werden. Sie benötigen weder einen physischen Server noch ein DBMS – beide werden für Sie von den Kaspersky-Experten gewartet.

Sie können Ihre verwalteten Geräte mit den Betriebssystemen Windows, Linux oder macOS unter die Kontrolle von Kaspersky Security Center Cloud Console migrieren. Wenn Ihr Netzwerk eine Administrationsserver-Hierarchie enthält, können Sie diese in Kaspersky Security Center Cloud Console speichern. Zusätzlich können Sie Folgendes übertragen:

- Aufgaben und Richtlinien verwalteter Programme
- Globale Aufgaben
- Benutzerdefinierte Geräteauswahlen
- Strukturen von Administrationsgruppen und darin enthaltene Geräte
- Tags, die den zu migrierenden Geräten zugewiesen wurden

Nach Abschluss der Migration können Sie die Geräte mit Kaspersky Security Center Cloud Console verwalten. Gleichzeitig bleiben die übertragenen Objekte erhalten und der Administrationsagent wird auf allen verwalteten Geräten neu installiert.

Weitere Informationen zur Durchführung der Migration und eine Liste der Voraussetzungen finden Sie in der *Hilfe von Kaspersky Security Center Cloud Console*.

Migration nach Kaspersky Next XDR Expert

Mithilfe dieses Szenarios können Sie die Struktur der Administrationsgruppe, einschließlich verwalteter Geräte und anderer Gruppenobjekte (Richtlinien, Aufgaben, globale Aufgaben, Tags und Geräteauswahlen) aus Kaspersky Security Center Windows unter die Verwaltung von Kaspersky Next XDR Expert übertragen.

Einschränkungen:

- Eine Migration von Kaspersky Security Center 14.2 Windows ist nur auf Kaspersky Next XDR Expert ab Version 1.0 möglich.
- Dieses Szenario kann nur unter Verwendung von Kaspersky Security Center Web Console durchgeführt werden.

Schritte

Die Migration durchläuft die die folgenden Schritte:

1. **Auswählen einer Migrationsmethode**

   Die Migration auf Kaspersky Next XDR Expert erfolgt mithilfe des Migrationsassistenten. Die Schritte des Migrationsassistenten hängen davon ab, ob die Administrationsserver von Kaspersky Security Center Windows und Kaspersky Next XDR Expert hierarchisch angeordnet sind:

   - Migration unter Verwendung einer Hierarchie von Administrationsservern

     Wählen Sie diese Option, wenn der Administrationsserver von Kaspersky Security Center Windows als sekundärer Administrationsserver von Kaspersky Next XDR Expert fungiert. Sie verwalten den Migrationsprozess und wechseln innerhalb der Konsole von Kaspersky Security Center zwischen Servern. Wenn Sie diese Option bevorzugen, können Sie die Administrationsserver in einer Hierarchie anordnen, um den Migrationsvorgang zu vereinfachen. Erstellen Sie dazu die Hierarchie, bevor Sie mit der Migration beginnen.

   - Migration mithilfe einer Exportdatei (zip-Archiv)

     Wählen Sie diese Option, wenn die Administrationsserver von Kaspersky Security Center Windows und Kaspersky Next XDR Expert nicht in einer Hierarchie angeordnet sind. Sie verwalten den Migrationsprozess mithilfe von zwei Konsolen: eine Konsole als Instanz für Kaspersky Security Center Windows und eine für Kaspersky Security Center. In diesem Fall verwenden Sie die Exportdatei, die Sie während des Exports aus Kaspersky Security Center Windows erstellt und heruntergeladen haben, und importieren diese Datei in Kaspersky Next XDR Expert.

2. **Daten aus Kaspersky Security Center Windows exportieren**

   Öffnen Kaspersky Security Center Windows und starten Sie anschließend den Migrationsassistenten.

3. **Daten in Kaspersky Next XDR Expert importieren**

   Fahren Sie mit dem Migrationsassistenten fort, um die exportierten Daten in Kaspersky Next XDR Expert zu importieren.

   Wenn die Server hierarchisch angeordnet sind, wird der Import nach einem erfolgreichen Export innerhalb desselben Assistenten automatisch gestartet. Wenn die Server nicht in einer Hierarchie angeordnet sind, fahren Sie nach dem Wechsel zu Kaspersky Next XDR Expert mit dem Migrationsassistenten fort.

4. **Ausführen zusätzlicher Aktionen, um Objekte und Einstellungen manuell von Kaspersky Security Center Windows nach Kaspersky Next XDR Expert zu übertragen (optionaler Schritt)**

   Möglicherweise möchten Sie auch die Objekte und Einstellungen übertragen, die nicht mithilfe des Migrationsassistenten übertragen werden können. Sie können beispielsweise folgende Vorgänge zusätzlich ausführen:

   - Globale Aufgaben des Administrationsservers konfigurieren
   - Richtlinieneinstellungen des Administrationsagenten konfigurieren
   - Installationspakete für Programme erstellen

- Virtuelle Server erstellen
- Verteilungspunkte zuweisen und konfigurieren
- Regeln für das Verschieben von Geräten konfigurieren
- Regeln für das automatische Zuweisen von Tags an Geräte konfigurieren
- Programmkategorien erstellen

5. **Die importierten verwalteten Geräte unter die Verwaltung von Kaspersky Next XDR Expert verschieben**

   Um die Migration abzuschließen, verschieben Sie die importierten verwalteten Geräte unter die Verwaltung von Kaspersky Next XDR Expert. Sie können dies auf eine der folgenden Arten tun:

   - Mittels einer Gruppenaufgabe von Kaspersky Security Center

     Verwenden Sie die Aufgabe Administrationsserver wechseln, um für bestimmte Client-Geräte zu einem anderen Administrationsserver zu wechseln.

   - Mithilfe des Tools klmover.

     Verwenden Sie das Tool "klmover" und geben Sie die Verbindungseinstellungen des neuen Administrationsservers an.

   - Mittels Installation oder Neuinstallation des Administrationsagenten auf den verwalteten Geräten

     Erstellen Sie ein neues Installationspaket des Administrationsagenten und geben Sie die Verbindungseinstellungen des neuen Administrationsservers in den Eigenschaften des Installationspakets an. Verwenden Sie das Installationspaket, um den Administrationsagenten mit einer Aufgabe zur Remote-Installation auf den importierten verwalteten Geräten zu installieren.

     Sie können auch ein autonomes Installationspaket erstellen und den Administrationsagenten mittels des Pakets lokal installieren.

6. **Administrationsagent auf die neueste Version aktualisieren**

   Es wird empfohlen, den Administrationsagenten zu aktualisieren, damit er dieselbe Version wie die Konsole von Kaspersky Security Center aufweist.

7. **Sicherstellen, dass die verwalteten Geräte auf dem neuen Administrationsserver sichtbar sind**

   Öffnen Sie auf dem Administrationsserver von Kaspersky Next XDR Expert die Liste der verwalteten Geräte (**Assets (Geräte)** → **Verwaltete Geräte**) und überprüfen Sie die Werte in den Spalten **Sichtbar**, **Administrationsagent ist installiert** und **Letzte Verbindung mit dem Administrationsserver**.

Weitere Methoden der Datenmigration

Neben dem Migrationsassistenten können Sie auch bestimmte Aufgaben und Richtlinien übertragen:

- Exportieren Sie die Aufgaben aus Kaspersky Security Center Windows und importieren Sie die Aufgaben anschließend in Kaspersky Next XDR Expert.
- Exportieren Sie die Richtlinien aus Kaspersky Security Center Windows und importieren Sie die Richtlinien anschließend in Kaspersky Next XDR Expert. Die zugehörigen Richtlinienprofile werden zusammen mit den ausgewählten Richtlinien exportiert und importiert.

Migration nach Kaspersky Security Center Linux

Die Migration von Kaspersky Security Center Windows zu Kaspersky Security Center Linux ist mittels Backup der Daten des Administrationsservers (mit dem Tool "klbackup") und mittels Migrationsassistent möglich.

In der folgenden Tabelle können Sie die wichtigsten Funktionen und Einschränkungen der Migration anhand der Daten des Administrationsservers und mittels des Migrationsassistenten vergleichen. Auf diese Weise können Sie entscheiden, welcher Ansatz für Ihre Organisation der passendere ist.

Parameter	Daten-Backup des Administrationsservers	Migrationsassistent
Migrationsprozess	Erstellen eines vollständigen Backups der Daten des Administrationsservers von Kaspersky Security Center Windows und Wiederherstellen des Backups auf einem Administrationsserver von Kaspersky Security Center Linux	Auswählen und Exportieren von Daten des Administrationsservers für die Migration, Importieren dieser Daten in den Administrationsserver von Kaspersky Security Center Linux und verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen
Merkmale der Migrationsmethode	• Migration aller Daten des Administrationsservers • Migration einer beliebigen Anzahl verwalteter Geräte • Wird verwendet, um eine vollständige Kopie des Administrationsservers von Kaspersky Security Center Windows zu erstellen und diese auf den Administrationsserver von Kaspersky Security Center Linux zu übertragen.	• Teilweise Migration der Daten des Administrationsservers • Zu migrierende Objekte können ausgewählt werden • Zu migrierende Administrationsgruppen oder Untergruppen können maximal 10.000 Geräte umfassen • Wird verwendet, um die Daten des Administrationsservers teilweise zu migrieren. Es werden nur Gruppenobjekte innerhalb des Migrationsbereichs migriert – Gruppenobjekte außerhalb des Migrationsbereichs müssen manuell wiederhergestellt werden.
Migrationsbereich	Vollständige Übertragung der Daten des Administrationsservers mit einer unbegrenzten Anzahl verwalteter Geräte	• Struktur der Administrationsgruppen • Verwaltete Geräte innerhalb von Administrationsgruppen (**max. 10.000 Geräte**) • Tags, zugewiesen an migrierende Geräte • Globale Aufgaben des Administrationsagenten und der verwalteten Anwendungen (nicht für Administrationsserver) • Gruppenaufgaben des Administrationsagenten und der verwalteten Anwendungen • Richtlinien verwalteter Anwendungen • Berichtsvorlagen • Benutzerrollen • Interne Benutzer und Sicherheitsgruppen • Benutzerdefinierte Programmkategorien mit manuell hinzugefügtem Inhalt • Benutzerdefinierte Geräteauswahlen
Nicht migrierter Bereich	—	• Globale Aufgaben des Administrationsservers • Auf dem Administrationsserver gespeicherte Ereignisse • Datenverwaltung der Programmpakete zur Remote-Installation • Zertifikat des Administrationsservers • Lizenzschlüssel, die vom Administrationsserver und von verwalteten Programmen verwendet werden • Virtuelle Administrationsserver • Richtlinieneinstellungen des Administrationsagenten • Verschiebungsregeln für Geräte • Regeln für das automatische Zuweisen von Tags an Geräte • Verteilungspunkte • Auf dem Administrationsserver gespeicherte Einstellungen von Kaspersky-Anwendungen
Unterstützte Versionen von Kaspersky Security Center	• Jede unterstützte Version von Kaspersky Security Center Windows • Kaspersky Security Center Linux Version 15.2 oder höher	• Kaspersky Security Center Windows Version 14.2 oder höher • Kaspersky Security Center Linux Version 15 oder höher
DBMSs, zwischen denen migriert werden kann	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (nur bei Migration von Kaspersky Security Center Windows Version 14.2 oder höher mit installiertem Patch zu Kaspersky Security Center Linux Version 15.3 oder höher) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (nur bei einer Migration von Kaspersky Security Center Windows Version 15.1 oder höher auf Kaspersky Security Center Linux Version 16 oder höher)	Uneingeschränkte Migration zwischen unterstützten DBMS

Migration auf Kaspersky Security Center Linux mittels Daten-Backups des Administrationsservers

Sie können ein Daten-Backup verwenden, um die Daten des Administrationsservers von Kaspersky Security Center Windows auf Kaspersky Security Center Linux zu migrieren. Stellen Sie vor der Migration sicher, dass die erforderlichen Funktionen von Kaspersky Security Center Windows durch Kaspersky Security Center Linux unterstützt werden.

Einschränkungen:

- Eine Migration ist zwischen den folgenden DBMS möglich:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Wenn die Daten des Administrationsservers in einer Microsoft SQL Server-, MySQL- oder MariaDB-Datenbank gespeichert werden, wird deren Migration zu MySQL oder MariaDB von jeder unterstützten Version von Kaspersky Security Center Windows auf Kaspersky Security Center Linux Version 15.2 oder höher unterstützt.
- Die Migration von Administrationsserverdaten, die in der PostgreSQL-Datenbank gespeichert sind, zu einer anderen PostgreSQL-Datenbank oder von einer Postgres Pro-Datenbank zu Postgres Pro wird von Kaspersky Security Center Windows Version 15.1 oder höher auf Kaspersky Security Center Linux Version 16 oder höher unterstützt.
- Wenn die Daten des Administrationsservers in einer Microsoft SQL Server-Datenbank gespeichert werden, wird deren Migration zu PostgreSQL oder Postgres Pro von Kaspersky Security Center Windows Version 14.2 oder höher auf Kaspersky Security Center Linux Version 15.2 oder höher unterstützt.

  Um die Migration zu PostgreSQL oder Postgres Pro zu unterstützen, haben Sie folgende Möglichkeiten:
  - Installieren Sie den Patch 15.1.0.20748-pf2 für den Kaspersky Security Center Windows Administrationsserver. Wenden Sie sich an den Technischen Support, um diesen Patch zu erhalten.
  - Aktualisieren Sie Kaspersky Security Center Windows auf Version 15.1.0.22239.
- Wenn Sie MySQL oder MariaDB als DBMS für Kaspersky Security Center Windows und für Kaspersky Security Center Linux verwenden, muss der Parameter `lower_case_table_names` für das aktuelle und das neue DBMS übereinstimmen.

  Überprüfen Sie daher den Parameter `lower_case_table_names`, bevor Sie ein Daten-Backup anlegen. Wenn Sie anschließend MySQL oder MariaDB für Kaspersky Security Center Linux installieren, müssen Sie für diesen Parameter denselben Wert angeben, der unter Windows für diesen Parameter angegeben war.

Schritte

Die Migration mittels Backup der Daten des Administrationsservers erfolgt schrittweise:

1. **Überprüfen, dass Sie über das interne Benutzerkonto des Administrators verfügen, mit dem Sie sich am Administrationsserver anmelden können.**

   Das Administratorkonto wird für die Anmeldung am Kaspersky Security Center Linux Administrationsserver verwendet. Wenn Sie nicht über dieses Konto verfügen und lediglich mit einem lokalen Windows-Konto oder einem Domänenkonto angemeldet sind, können Sie sich nach der Wiederherstellung des Backups nicht beim Kaspersky Security Center Linux Administrationsserver anmelden. Vom Kaspersky Security Center Linux Administrationsserver wird das Anmelden mit einem lokalen Windows-Konto nicht unterstützt. Das Anmelden mit einem Domänenkonto ist möglich, erfordert aber möglicherweise eine zusätzliche Konfiguration des Administrationsservers.

   Wenn Sie kein Administratorkonto besitzen, müssen Sie dieses Konto nach dem Wiederherstellen der Backup-Kopie mithilfe des Tools "kladduser" erstellen.

2. **Eine aktuelle Backup-Kopie der Daten des Administrationsservers von Kaspersky Security Center Windows erstellen**

   Je nachdem, welches DBMS Sie für Kaspersky Security Center Windows und Kaspersky Security Center Linux verwenden, führen Sie einen der folgenden Schritte aus:

   - Bei einer Migration von MySQL oder MariaDB auf MySQL oder MariaDB: Legen Sie eine Backup-Kopie anhand des Tools klbackup oder der Aufgabe Anlegen eines Daten-Backups auf dem Gerät mit dem installierten Administrationsserver an.
   - Bei einer Migration von PostgreSQL auf PostgreSQL und von PostgreSQL Pro auf PostgreSQL Pro: Erstellen Sie auf dem Gerät mit dem installierten Administrationsserver eine Backup-Kopie mittels des Tools klbackup oder der Aufgabe zum Anlegen eines Backups.
   - Bei einer Migration von Microsoft SQL Server auf MySQL oder MariaDB: Erstellen Sie ein Backup mittels des Tools klbackup mit aktivierter Option **Auf MySQL/MariaDB-Format migrieren**.
   - Bei einer Migration von Microsoft SQL Server zu PostgreSQL oder Postgres Pro:

     1. Fordern Sie beim Technischen Support von Kaspersky den Patch 15.1.0.20748-pf2 für den Administrationsserver an und installieren Sie ihn anschließend, um die Migration zu PostgreSQL und Postgres Pro zu unterstützen.

        Alternativ können Sie Kaspersky Security Center Windows auf Version 15.1.0.22239 aktualisieren.

     2. Erstellen Sie ein Backup mittels des Tools "klbackup".

        Wenn Sie klbackup über die Befehlszeile ausführen, verwenden Sie das Flag `-migrate postgres`.

        Wenn Sie die Benutzeroberfläche von klbackup verwenden, aktivieren Sie die Option **Auf Postgres-Format migrieren**.

   Trennen Sie nach dem Erstellen der Backup-Kopie den Administrationsserver von Kaspersky Security Center Windows vom Netzwerk.

3. **Ein neues Gerät auf die Installation von Kaspersky Security Center Linux vorbereiten**

Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

1. Wählen Sie ein neues Gerät, auf dem der Administrationsserver installiert werden soll. Dieses Gerät muss die Hard- und Softwarevoraussetzungen erfüllen. Überprüfen Sie auch, ob die auf dem Administrationsserver verwendeten Ports verfügbar sind.

2. Weisen Sie dem neuen Gerät dieselbe Adresse zu.

   Dem neuen Administrationsserver können der NetBIOS-Name, der FQDN und die statische IP-Adresse zugewiesen werden. Dies hängt davon ab, welche Adresse für den Administrationsagenten im Installationspaket des Administrationsagenten angegeben wurde, als die Administrationsagenten verteilt wurden. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools klnagchk ermittelt werden).

4 DBMS installieren und konfigurieren

Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

1. Wählen Sie den DBMS-Typ aus, der die optimale Leistung bietet. Berücksichtigen Sie dabei die Anzahl der vernetzten Geräte, die Netzwerktopologie und die Netzwerkauslastung. Sie können eines der unterstützten DBMS auswählen.

2. Installieren Sie das DBMS gemäß dem DBMS-Typ, der beim Anlegen des Backups ausgewählt wurde. Informationen zur Installation des ausgewählten DBMS finden Sie in der DBMS-Dokumentation.

   > Die neue Datenbankversion darf nicht niedriger sein als die aktuelle Version.

3. Konfigurieren Sie das DBMS für die Verwendung mit Kaspersky Security Center Linux

5 Kaspersky Security Center Linux installieren

Installieren Sie Kaspersky Security Center Linux auf dem neuen Gerät:

Das während der Installation erstellte interne Benutzerkonto des Administrators geht ebenso wie andere Objekte (Gruppen, Richtlinien, Aufgaben, Benutzer), die Sie vor der Wiederherstellung der Administrationsserverdaten aus dem Backup erstellt haben, nach der Wiederherstellung verloren. Diese Objekte werden durch Objekte ersetzt, die im Backup enthalten sind.

6 Daten des Administrationsservers aus der Backup-Kopie wiederherstellen

Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

1. Stellen Sie die Daten des Administrationsservers auf dem neuen Gerät mithilfe des Tools klbackup wieder her.

2. Wenn Sie nicht über das interne Benutzerkonto des Administrators, mit dem Sie sich am Kaspersky Security Center Administrationsserver angemeldet haben, verfügten und Sie ein lokales Windows-Konto oder ein Domänenkonto verwendet haben, nutzen Sie das Tool "kladduser", um wie folgt ein Administratorkonto zu erstellen:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

wobei der Parameter `<password>` die folgenden Anforderungen erfüllen muss:

- Das Benutzerkennwort muss mindestens 8 Zeichen und darf maximal 256 Zeichen enthalten.
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Ziffern (0–9)
  - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Server der Web Console von Kaspersky Security Center installieren und Administrationsserver konfigurieren**

   Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

   1. Installieren Sie Kaspersky Security Center Web Console.

      Wenn die Kaspersky Security Center Web Console bereits installiert ist, installieren Sie die Web Console mit der gleichen Antwortdatei erneut.

      Melden Sie sich mit dem internen Benutzerkonto des Administrators an der Kaspersky Security Center Web Console an.

      Nach der Wiederherstellung der Daten des Administrationsservers dauert die Dateninitialisierung normalerweise bis zu 15 Minuten. Die genaue Zeit ist jedoch von der Hardwareleistung und der Größe der Daten des Administrationsservers abhängig. Während dieser Zeit kann die Kaspersky Security Center Web Console möglicherweise keine Verbindung herstellen und zeigt entsprechende Fehler an.

   2. Nachdem die Dateninitialisierung in der Datenbank abgeschlossen ist, überprüfen Sie die Funktionstüchtigkeit der Hauptfunktionen des Administrationsservers. Stellen Sie sicher, dass sich der Administrationsserver mit den verwalteten Geräten synchronisiert und dass die Daten des Administrationsservers wiederhergestellt wurden.

   3. Fragen Sie die Domänencontroller ab, um Informationen über die Domänenstruktur, Benutzerkonten, Sicherheitsgruppen und DNS-Namen jener Geräte wiederherzustellen, die zur Domäne gehören.

   4. Deinstallieren Sie bei Bedarf den Administrationsserver und den Datenbankserver vom bisherigen Gerät.

      Innerhalb eines Netzwerks dürfen sich nicht mehrere Administrationsserver mit gleicher Verbindungsadresse und gleichem Administrationsserver-Zertifikat befinden.

Der Administrator hat Zugriff auf die Daten des Administrationsservers und auf die verwalteten Geräte, die in Kaspersky Security Center Windows verfügbar waren. Dies gilt jedoch unter der Einschränkung, dass die erforderlichen Funktionen in Kaspersky Security Center Linux unterstützt werden.

Migration zu Kaspersky Security Center Linux mittels Migrationsassistenten

Mithilfe dieses Szenarios können Sie die Struktur der Administrationsgruppe, einschließlich verwalteter Geräte und anderer Gruppenobjekte (Richtlinien, Aufgaben, globale Aufgaben, Tags und Geräteauswahlen) aus Kaspersky Security Center Windows unter die Verwaltung von Kaspersky Security Center Linux übertragen. Stellen Sie vor der Migration sicher, dass die erforderlichen Funktionen von Kaspersky Security Center Windows durch Kaspersky Security Center Linux unterstützt werden.

Einschränkungen:

- Eine Migration ist nur von Kaspersky Security Center Windows ab Version 14.2 zu Kaspersky Security Center Linux ab Version 15 möglich.
- Dieses Szenario kann nur unter Verwendung von Kaspersky Security Center Web Console durchgeführt werden.

Schritte

Die Migration durchläuft die die folgenden Schritte:

1. **Auswählen einer Migrationsmethode**

   Die Migration auf Kaspersky Security Center Linux erfolgt mithilfe des Migrationsassistenten. Die Schritte des Migrationsassistenten hängen davon ab, ob die Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux hierarchisch angeordnet sind:

   - Migration unter Verwendung einer Hierarchie von Administrationsservern

     Wählen Sie diese Option, wenn der Administrationsserver für Kaspersky Security Center Windows als sekundärer Administrationsserver für Kaspersky Security Center Linux fungiert. Sie verwalten den Migrationsprozess und wechseln zwischen Servern innerhalb einer einzigen Instanz der Kaspersky Security Center Web Console. Wenn Sie diese Option bevorzugen, können Sie die Administrationsserver in einer Hierarchie anordnen, um den Migrationsvorgang zu vereinfachen. Erstellen Sie dazu die Hierarchie, bevor Sie mit der Migration beginnen.

   - Migration mithilfe einer Exportdatei (zip-Archiv)

     Wählen Sie diese Option, wenn die Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux nicht in keiner Hierarchie angeordnet sind. Sie verwalten den Migrationsprozess mit zwei Instanzen der Kaspersky Security Center Web Console – eine Instanz für Kaspersky Security Center Windows und eine weitere für Kaspersky Security Center Linux. In diesem Fall verwenden Sie die Exportdatei, die Sie während des Exports aus Kaspersky Security Center Windows erstellt und heruntergeladen haben, und importieren diese Datei in Kaspersky Security Center Linux.

2. **Sichern Sie das Zertifikat und den privaten Schlüssel des Administrationsservers für Kaspersky Security Center Windows (optionaler Schritt)**

   Sie können die verwalteten Geräte unter die Verwaltung des Administrationsservers von Kaspersky Security Center Linux stellen, indem Sie das Zertifikat und den privaten Schlüssel des Administrationsservers aus einer Backup-Kopie wiederherstellen. Erstellen Sie in diesem Fall ein Backup des Zertifikats und privaten Schlüssels des Administrationsservers für Kaspersky Security Center Windows. Stellen Sie anschließend im Schritt 6 das Zertifikat und den privaten Schlüssel wieder her.

3. **Daten aus Kaspersky Security Center Windows exportieren**

   Öffnen Kaspersky Security Center Windows und starten Sie anschließend den Migrationsassistenten.

4. **Daten in Kaspersky Security Center Linux importieren**

   Fahren Sie mit dem Migrationsassistenten fort, um die exportierten Daten in Kaspersky Security Center Linux zu importieren. Wenn die Server hierarchisch angeordnet sind, wird der Import nach einem erfolgreichen Export innerhalb desselben Assistenten automatisch gestartet. Wenn die Server nicht in einer Hierarchie angeordnet sind, fahren Sie nach dem Wechsel zu Kaspersky Security Center Linux mit dem Migrationsassistenten fort.

5. **Ausführen zusätzlicher Aktionen, um Objekte und Einstellungen manuell von Kaspersky Security Center Windows nach Kaspersky Security Center Linux zu übertragen (optionaler Schritt)**

Möglicherweise möchten Sie auch die Objekte und Einstellungen übertragen, die nicht mithilfe des Migrationsassistenten übertragen werden können. Sie können beispielsweise folgende Vorgänge zusätzlich ausführen:

- Übertragen der Lizenzschlüssel, die vom Administrationsserver und von verwalteten Programmen verwendet werden
- Konfigurieren der globalen Aufgaben des Administrationsservers
- Richtlinieneinstellungen des Administrationsagenten konfigurieren
- Installationspakete für Programme erstellen
- Virtuelle Server erstellen
- Verteilungspunkte zuweisen und konfigurieren
- Regeln für das Verschieben von Geräten konfigurieren
- Regeln für das automatische Zuweisen von Tags an Geräte konfigurieren
- Programmkategorien erstellen

6. **Die importierten verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux verschieben**

Um die Migration abzuschließen, verschieben Sie die importierten verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux. Sie können dies auf eine der folgenden Arten tun:

- Mithilfe des Tools klmover

  Verwenden Sie das Tool "klmover" und geben Sie die Verbindungseinstellungen des neuen Administrationsservers an.

- Mittels der Aufgabe *Administrationsserver ändern*

  Erstellen Sie die Aufgabe *Administrationsserver ändern* und geben Sie dabei die importierten verwalteten Geräte, den neuen Administrationsserver und weitere Aufgabeneinstellungen an. Führen Sie anschließend die Aufgabe aus, um die verwalteten Geräte unter Verwaltung des Administrationsservers für Kaspersky Security Center Linux zu stellen.

- Durch Deinstallation (bei bereits installierten) und weitere Installation des Administrationsagenten auf den verwalteten Geräten

  Erstellen Sie ein neues Installationspaket des Administrationsagenten und geben Sie die Verbindungseinstellungen des neuen Administrationsservers in den Eigenschaften des Installationspakets an. Deinstallieren Sie den Administrationsagenten auf den importierten verwalteten Geräten und verwenden Sie anschließend das erstellte Installationspaket, um den Administrationsagenten auf den importierten verwalteten Geräten mittels einer Aufgabe zur Remote-Installation zu installieren. Sie können auch ein autonomes Installationspaket erstellen und den Administrationsagenten mittels des Pakets lokal installieren. Weitere Informationen finden Sie unter Verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen.

- Durch das Wiederherstellung des Zertifikats und privaten Schlüssels des Administrationsservers aus einer Backup-Kopie (nur für die Migration auf Kaspersky Security Center Linux 15.1 oder höher).

  Weisen Sie dem Gerät mit dem Administrationsserver für Kaspersky Security Center Linux dieselbe Netzwerkadresse zu wie dem Administrationsserver für Kaspersky Security Center Windows. Führen Sie das Tool klbackupmit dem Parameter `-cert_only` aus, um das Zertifikat des Administrationsservers und den privaten Schlüssel aus der Backup-Kopie wiederherzustellen, die Sie in Schritt 2 gespeichert haben. Führen Sie in der Befehlszeile den folgenden Befehl aus: `/opt/kaspersky/ksc64/sbin/klbackup -path <Pfad zur Backup-Kopie des Administrationsserver-Zertifikats> -restore -cert_only`. Weitere Informationen dazu finden Sie unter Verwenden des klbackup-Tools, um verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers zu stellen.

7. **Administrationsagent auf die neueste Version aktualisieren**

   Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center.

8. **Sicherstellen, dass die verwalteten Geräte auf dem neuen Administrationsserver sichtbar sind**

   Öffnen Sie auf dem Administrationsserver mit Kaspersky Security Center Linux die Liste der verwalteten Geräte (**Assets (Geräte)** → **Verwaltete Geräte**) und überprüfen Sie die Werte in den Spalten **Sichtbar**, **Administrationsagent ist installiert** und **Letzte Verbindung mit dem Administrationsserver**.

Weitere Methoden der Datenmigration

Neben dem Migrationsassistenten können Sie auch bestimmte Aufgaben und Richtlinien übertragen:

- Exportieren Sie die Aufgaben aus Kaspersky Security Center Windows und importieren Sie die Aufgaben anschließend in Kaspersky Security Center Linux.
- Exportieren Sie bestimmte Richtlinien aus Kaspersky Security Center Windows und importieren Sie die Richtlinien anschließend in Kaspersky Security Center Linux. Die zugehörigen Richtlinienprofile werden zusammen mit den ausgewählten Richtlinien exportiert und importiert.

Gruppenobjekte aus Kaspersky Security Center Windows exportieren

Für die Migration der Struktur der Administrationsgruppe einschließlich verwalteter Geräte und anderer Gruppenobjekte von Kaspersky Security Center Windows auf Kaspersky Security Center Linux müssen Sie zuerst die Daten für den Export auswählen und eine Exportdatei erstellen. Die Exportdatei enthält Informationen über alle Gruppenobjekte, die Sie migrieren möchten. Die Exportdatei wird für den anschließenden Import in Kaspersky Security Center Linux verwendet.

Sie können die folgenden Objekte exportieren:

- Aufgaben und Richtlinien verwalteter Anwendungen
- Globale Aufgaben
- Benutzerdefinierte Geräteauswahlen
- Strukturen von Administrationsgruppen und darin enthaltene Geräte
- Tags, die den zu migrierenden Geräten zugewiesen wurden

Bevor Sie mit dem Export beginnen, machen Sie sich mit den allgemeine Informationen zur Migration auf Kaspersky Security Center Linux vertraut. Wählen Sie die Migrationsmethode – mit oder ohne Verwendung der Hierarchie der Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux.

So exportieren Sie verwaltete Geräte und zugehörige Gruppenobjekte über den Migrationsassistenten:

1. Je nachdem, ob sich der Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux in einer Hierarchie befinden, führen Sie einen der folgenden Schritte aus:

   - Wenn sich die Server in einer Hierarchie befinden, öffnen Sie die Kaspersky Security Center Web Console und wechseln Sie anschließend zum Server von Kaspersky Security Center Windows.

   - Wenn sich die Server nicht in einer Hierarchie befinden, öffnen Sie die Kaspersky Security Center Web Console, die mit Kaspersky Security Center Windows verbunden ist.

2. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Migration**.

3. Um den Assistenten zu starten und seine Schritte auszuführen, wählen Sie aus, wo Sie Ihre Daten und Einstellungen hin übertragen möchten.

   - Wenn Sie Ihre Daten und Einstellungen zu Kaspersky Security Center Cloud Console übertragen möchten, wählen Sie die Option **Zu Kaspersky Security Center Cloud Console migrieren** aus.

   - Wenn Sie Ihre Daten und Einstellungen zu Kaspersky Security Center Linux oder Kaspersky Next XDR Expert übertragen möchten, wählen Sie **Zu Kaspersky Security Center Linux oder auf die Open Single Management Platform migrieren** aus.

4. Wählen Sie die Administrationsgruppe oder Untergruppe aus, die Sie exportieren möchten. Bitte stellen Sie sicher, dass die ausgewählte Administrationsgruppe oder Untergruppe nicht mehr als 10.000 Geräte umfasst.

5. Wählen Sie die verwalteten Anwendungen aus, deren Aufgaben und Richtlinien exportiert werden. Wählen Sie nur Anwendungen aus, die auch von Kaspersky Security Center Linux unterstützt werden. Die Objekte von nicht unterstützten Anwendungen werden zwar auch exportiert, sind aber nicht nutzbar.

6. Verwenden Sie die Links auf der linken Seite, um die globalen Aufgaben, die Geräteauswahlen und die zu exportierenden Berichte auszuwählen. Mit dem Link **Gruppenobjekte** können Sie folgende Objekte vom Export ausschließen: benutzerdefinierte Rollen, interne Benutzer und Sicherheitsgruppen sowie benutzerdefinierte Programmkategorien.

Die Exportdatei (zip-Archiv) wird erstellt. Abhängig davon, ob Sie die Migration mit Unterstützung der Hierarchie der Administrationsserver durchführen oder nicht, wird die Exportdatei wie folgt gespeichert:

- Wenn die Server in einer Hierarchie angeordnet sind, wird die Exportdatei im temporären Ordner des Servers der Web Console von Kaspersky Security Center gespeichert.

- Wenn die Server nicht in einer Hierarchie angeordnet sind, wird die Exportdatei auf Ihr Gerät heruntergeladen.

Bei einer Migration mit Unterstützung der Hierarchie der Administrationsserver startet der Import automatisch nach einem erfolgreichen Export. Für die Migration ohne Unterstützung der Hierarchie der Administrationsserver können Sie die gespeicherte Exportdatei manuell in Kaspersky Security Center Linux importieren.

Importieren der Exportdatei in Kaspersky Security Center Linux

Um aus Kaspersky Security Center Windows exportierte Informationen zu verwalteten Geräten und Objekten mitsamt deren Einstellungen zu übertragen, müssen Sie diese in Kaspersky Security Center Linux oder Kaspersky Next XDR Expert importieren.

So importieren Sie verwaltete Geräte und zugehörige Gruppenobjekte über den Migrationsassistenten:

1. Je nachdem, ob sich Administrationsserver von Kaspersky Security Center Windows und Kaspersky Security Center Linux in einer Hierarchie befinden, führen Sie einen der folgenden Schritte aus:

   - Wenn die Server in einer Hierarchie angeordnet sind, fahren Sie nach Abschluss des Exports mit dem nächsten Schritt des Migrationsassistenten fort. Der Import wird nach einem erfolgreichen Export innerhalb dieses Assistenten automatisch gestartet (siehe Schritt 2 dieser Anleitung).

   - Wenn die Server in keiner Hierarchie angeordnet sind:

     a. Öffnen Sie die Kaspersky Security Center Web Console, die mit Kaspersky Security Center Linux oder Kaspersky Next XDR Export verbunden ist.

     b. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Migration**.

     c. Wählen Sie die Exportdatei (zip-Archiv) aus, die Sie während des Exports aus Kaspersky Security Center Windows erstellt und heruntergeladen haben. Das Hochladen der Exportdatei wird gestartet.

2. Nachdem die Exportdatei erfolgreich hochgeladen wurde, können Sie den Import fortsetzen. Wenn Sie eine andere Exportdatei angeben möchten, klicken Sie auf den Link **Ändern** und wählen Sie die gewünschte Datei aus.

3. Es wird die gesamte Hierarchie der Administrationsgruppen von Kaspersky Security Center Linux wird angezeigt.

   Aktivieren Sie das Kontrollkästchen neben der Ziel-Administrationsgruppe, für welche die Objekte der exportierten Administrationsgruppe (verwaltete Geräte, Richtlinien, Aufgaben und weitere Gruppenobjekte) wiederhergestellt werden sollen.

4. Der Import der Gruppenobjekte wird gestartet. Sie können den Migrationsassistenten während des Imports nicht minimieren und keine gleichzeitigen Vorgänge ausführen. Warten Sie, bis alle Aktualisierungssymbole (🔄) neben den Elementen der Objektliste durch grüne Häkchen (✓) ersetzt wurden und der Import beendet ist.

5. Nach Abschluss des Imports wird die exportierte Struktur der Administrationsgruppen einschließlich der Gerätedetails unter der von Ihnen ausgewählten Ziel-Administrationsgruppe angezeigt. Wenn der Name des wiederherzustellenden Objekts mit dem Namen eines bereits vorhandenen Objekts identisch ist, besitzt das wiederhergestellte Objekt ein inkrementelles Suffix.

> Wenn in einer migrierten Aufgabe die Details des Benutzerkontos angegeben sind, mit dem die Aufgabe ausgeführt wird, müssen Sie die Aufgabe öffnen und das Kennwort nach Abschluss des Imports erneut eingeben.

Wenn der Import mit einem Fehler abgeschlossen wurde, können Sie eine der folgenden Maßnahmen ergreifen:

- Für eine Migration mit unterstützter Hierarchie des Administrationsservers können Sie den Import der Exportdatei erneut starten.
- Für eine Migration ohne unterstützte Hierarchie des Administrationsservers können Sie den Migrationsassistenten starten, um eine andere Exportdatei auszuwählen und anschließend erneut zu importieren.

Sie können kontrollieren, ob die im Exportbereich enthaltenen Gruppenobjekte erfolgreich in Kaspersky Security Center Linux importiert wurden. Wechseln Sie dazu in den Abschnitt **Assets (Geräte)** und stellen Sie sicher, dass die importierten Objekte in den entsprechenden Unterabschnitten erscheinen.

Beachten Sie, dass die importierten verwalteten Geräte im Unterabschnitt **Verwaltete Geräte** zwar angezeigt werden, aber weder im Netzwerk sichtbar sind, noch dass der Administrationsagent auf ihnen installiert ist und ausgeführt wird (in den folgenden Spalten steht der Wert *Nein*: **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt**).

Um die Migration abzuschließen, müssen Sie die verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen.

Verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen

Nach dem in Kaspersky Security Center Linux die Informationen über verwaltete Geräte, Objekte und deren Einstellungen erfolgreich importiert wurden, müssen Sie die verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen, um die Migration abzuschließen.

Sie können die verwalteten Geräte auf eine der folgenden Arten unter die Verwaltung von Kaspersky Security Center Linux verschieben:

- Mittels des Tools Tool klmover.
- Mittels der Aufgabe *Administrationsserver ändern*.
- Mittels der Wiederherstellung des Zertifikats und privaten Schlüssels des Administrationsservers aus einer Backup-Kopie (nur für die Migration auf Kaspersky Security Center Linux 15.1 oder höher).

  Weitere Informationen dazu finden Sie in Schritt 6 des Hauptszenarios für die Migration.
- Mittels Aufgabe zur Remote-Installation durchgeführte Installation des Administrationsagenten auf dem verwalteten Gerät.

So stellen Sie die verwalteten Geräte mithilfe der Installation des Administrationsagenten unter Verwaltung von Kaspersky Security Center Linux:

1. Entfernen Sie den Administrationsagenten auf den importierten verwalteten Geräten, die unter die Verwaltung von Kaspersky Security Center Linux gestellt werden sollen.
2. Wechseln Sie zum Administrationsserver für Kaspersky Security Center Windows.
3. Gehen Sie zu **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete** und öffnen Sie die Eigenschaften eines existierenden Pakets des Administrationsagenten.

   Wenn in der Paketliste kein Installationspaket eines Administrationsagenten vorhanden ist laden Sie ein neues herunter.

Sie können auch ein autonomes Installationspaket erstellen und den Administrationsagenten mittels des Pakets lokal installieren.

4. Wählen Sie auf der Registerkarte **Einstellungen** den Abschnitt **Verbindung**. Geben Sie die Verbindungseinstellungen des Administrationsservers für Kaspersky Security Center Linux an.

5. Erstellen Sie eine Aufgabe zur Remote-Installation für importierte verwaltete Geräte und geben Sie anschließend das neu konfigurierte Installationspaket des Administrationsagenten an.

   Sie können den Administrationsagenten entweder über den Administrationsserver für Kaspersky Security Center Windows oder über ein Windows-Gerät installieren, das als Verteilungspunkt fungiert. Wenn Sie den Administrationsserver verwenden, aktivieren Sie die Option **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Wenn Sie einen Verteilungspunkt verwenden, aktivieren Sie die Option **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**.

6. Starten Sie die Aufgabe zur Remote-Installation des Programms.

Nachdem die Aufgabe zur Remote-Installation erfolgreich abgeschlossen wurde, wechseln Sie zum Administrationsserver für Kaspersky Security Center Linux und stellen Sie sicher, dass die verwalteten Geräte im Netzwerk sichtbar sind und dass der Administrationsagent auf ihnen installiert ist und ausgeführt wird (in folgenden Spalten muss der Wert auf *Ja* stehen: **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt**).

In der Kaspersky Security Center Web Console anmelden und abmelden

Sie können sich in der Kaspersky Security Center Web Console anmelden, nachdem Sie den Administrationsserver und den Server der Web Console installiert haben. Sie müssen die während der Installation angegebene Webadresse des Administrationsservers und den Port kennen (der Standard-Port ist 8080). In Ihrem Browser muss JavaScript aktiviert sein.

Sie können sich mit den folgenden Methoden an der Kaspersky Security Center Web Console anmelden:

- Mittels Domänenauthentifizierung

  Wenn Sie diese Methode wählen, stellen Sie sicher, dass die Abfrage des Domänencontrollers aktiviert ist und die Domänenbenutzer dem Administrationsserver hinzugefügt wurden.

- Mittels Eingabe von Name und Kennwort des Domänenbenutzers

- Mittels Eingabe von Benutzername und Passwort des Administrators

Das Benutzerkonto, mit dem Sie sich an der Kaspersky Security Center Web Console anmelden möchten, muss eine zugewiesene Rolle besitzen. Stellen Sie vor der Anmeldung sicher, dass der Domäne oder dem internen Benutzerkonto eine Rolle zugewiesen wurde. Andernfalls tritt ein Anmeldefehler auf.

Anmelden mittels Domänenauthentifizierung

So melden Sie sich mittels Domänenauthentifizierung an der Kaspersky Security Center Web Console an:

1. Rufen Sie in Ihrem Browser die folgende Adresse auf: https://<Adresse der Kaspersky Security Center Web Console>:<Port-Nummer>

   Die Anmeldeseite wird angezeigt.

2. Wenn Sie mehrere vertrauenswürdige Server hinzugefügt haben, wählen Sie in der Liste mit Administrationsservern den Administrationsserver aus, zu dem Sie eine Verbindung herstellen möchten.

   Wenn Sie nur einen einzigen Administrationsserver hinzugefügt haben, wird die Liste mit Administrationsservern nicht angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Domänenauthentifizierung verwenden**.
   - Wenn auf dem Server mindestens ein virtueller Administrationsserver erstellt wurde und Sie sich an einem virtuellen Server mittels Domänenauthentifizierung anmelden möchten:

     a. Klicken Sie auf die Schaltfläche **Optionen des virtuellen Servers anzeigen**.

     b. Geben Sie den Namen des virtuellen Administrationsservers ein, den Sie während der Erstellung des virtuellen Servers angegeben haben.

     c. Klicken Sie auf die Schaltfläche **Domänenauthentifizierung verwenden**.

4. Wenn für Ihr Konto die zweistufige Überprüfung aktiviert ist, geben Sie den Sicherheitscode an, der von der Authenticator-App auf dem mobilen Gerät generiert wurde.

   Bei Bedarf können Sie können zur Anmeldeseite zurückkehren.

Nach der Anmeldung wird das Dashboard in der Sprache und dem Design angezeigt, das Sie zuletzt verwendet haben. Sie können in der Kaspersky Security Center Web Console navigieren und sie bei Ihrer Arbeit mit Kaspersky Security Center nutzen.

Anmeldung mittels Eingabe des Benutzernamens und Kennworts des Administrators

So melden Sie sich mittels Eingabe des Benutzernamens und Passworts des Administrators an der Kaspersky Security Center Web Console an:

1. Rufen Sie in Ihrem Browser die folgende Adresse auf: https://<Adresse der Kaspersky Security Center Web Console>:<Port-Nummer>

   Die Anmeldeseite wird angezeigt.

2. Wenn Sie mehrere vertrauenswürdige Server hinzugefügt haben, wählen Sie in der Liste mit Administrationsservern den Administrationsserver aus, zu dem Sie eine Verbindung herstellen möchten.

   Wenn Sie nur einen einzigen Administrationsserver hinzugefügt haben, wird die Liste mit Administrationsservern nicht angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - So melden Sie sich am Administrationsserver mit dem Konto eines Domänenbenutzers an:

     a. Geben Sie den Namen und das Kennwort des Domänenbenutzers an.

     Sie können den Benutzernamen des Domänenbenutzers in einem der folgenden Formate eingeben:

     - `Benutzername@dns.domain`
     - `NTDOMAIN\Benutzername`

     b. Klicken Sie auf die Schaltfläche **Anmelden**.

     Bevor Sie sich mit dem Konto eines Domänenbenutzers anmelden, fragen Sie den Domänencontroller ab, um die Liste der Domänenbenutzer abzurufen.

   - So melden Sie sich am Administrationsserver an:

     a. Geben Sie den Benutzernamen und das Kennwort des lokalen Administrators ein.

     b. Klicken Sie auf die Schaltfläche **Anmelden**.

   - Wenn auf dem Server mindestens ein virtueller Administrationsserver erstellt wurde und Sie sich an einem virtuellen Server anmelden möchten:

     a. Klicken Sie auf die Schaltfläche **Optionen des virtuellen Servers anzeigen**.

     b. Geben Sie den Namen des virtuellen Administrationsservers ein, den Sie während der Erstellung des virtuellen Servers angegeben haben.

     c. Geben Sie den Benutzernamen und das Passwort des Administrators ein, der die Berechtigungen für den virtuellen Administrationsserver besitzt.

     d. Klicken Sie auf die Schaltfläche **Anmelden**.

4. Wenn für Ihr Konto die zweistufige Überprüfung aktiviert ist, geben Sie den Sicherheitscode an, der von der Authenticator-App auf dem mobilen Gerät generiert wurde.

   Bei Bedarf können Sie können zur Anmeldeseite zurückkehren.

5. Wenn für Ihr Konto die erzwungene Kennwortänderung aktiviert ist oder Ihr Kennwort abgelaufen ist, wird das Fenster zur Kennwortänderung angezeigt. Legen Sie ein neues Kennwort fest, um sich an der Kaspersky Security Center Web Console anzumelden.

Nach der Anmeldung wird das Dashboard in der Sprache und dem Design angezeigt, das Sie zuletzt verwendet haben. Sie können in der Kaspersky Security Center Web Console navigieren und sie bei Ihrer Arbeit mit Kaspersky Security Center nutzen.

Abmelden

So melden Sie sich von einer laufenden Sitzung der Kaspersky Security Center Web Console ab:

Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Abmelden.**

Kaspersky Security Center Web Console wird beendet und die Anmeldeseite wird angezeigt.

Identitäts- und Zugriffsverwaltung in Kaspersky Security Center Web Console

Dieser Abschnitt enthält Informationen zur Identitäts- und Zugriffsverwaltung (auch als IAM bezeichnet).

Über die Identitäts- und Zugriffsverwaltung

Die *Identitäts- und Zugriffsverwaltung* (auch IAM genannt) ist eine Komponente der Kaspersky Security Center Web Console, welche die Verwendung von Single Sign-On (SSO) zwischen der Kaspersky Security Center Web Console und der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks ermöglicht. IAM verwendet das OAuth 2.0-Protokoll, um die Autorisierung von Kaspersky Industrial CyberSecurity for Networks an der Kaspersky Security Center Web Console sicherzustellen.

In diesem Fall wird Kaspersky Industrial CyberSecurity for Networks, auf welches Sie über die Kaspersky Security Center Web Console Zugriff erhalten, als *Ressourcenserver* bezeichnet, und die Kaspersky Security Center Web Console sowie die Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks als *OAuth 2.0-Clients*. Ein Ressourcenserver ist ein Programm, das mit mehreren Benutzern arbeitet und eine Autorisierung erfordert. Der Client verwendet für die Autorisierung auf dem Ressourcenserver einen *Token*. Ein Token ist eine eindeutige Folge von Bytes. Wenn ein Token abläuft, wird es automatisch neu ausgestellt. IAM fungiert als einzelner Autorisierungsserver für mehrere OAuth 2.0-Clients.

Sie können IAM bei der Installation von Kaspersky Security Center Web Console installieren. Sie können es später jederzeit in den Einstellungen der Kaspersky Security Center Web Console aktivieren. Wenn der Server oder die Web-Oberfläche von Kaspersky Industrial CyberSecurity auf einem Gerät installiert sind, dass vom gleichen Administrationsserver verwaltet wird, erkennt IAM dieses Programm und in der Kaspersky Security Center Web Console wird eine Benachrichtigung angezeigt, die Sie darüber informiert. Sie können Kaspersky Industrial CyberSecurity for Networks registrieren und SSO später sowohl für die Kaspersky Security Center Web Console als auch für die Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks verwenden.

Wenn Sie sich von der Kaspersky Security Center Web Console abmelden, wird Ihre Sitzung in der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks beendet und Sie müssen sich bei der Kaspersky Security Center Web Console erneut anmelden.

Aktivieren der Identitäts- uns Zugriffsverwaltung: Szenario

Erforderliche Vorrausetzungen

Stellen Sie vor Beginn sicher, dass Sie Zugriff auf Kaspersky Industrial CyberSecurity for Networks Version 3.1 oder höher haben.

Schritte

Die Aktivierung der Identitäts- und Zugriffsverwaltung (auch als IAM bezeichnet) erfolgt in Stufen:

1. **Überprüfen der erforderlichen Ports**

   Stellen Sie sicher, dass die Ports 3333, 4004 und 4444 auf dem Gerät geöffnet sind, auf dem Kaspersky Security Center Web Console installiert ist. Diese Ports werden für die Verwendung von OAuth 2.0 benötigt. Bei Bedarf können Sie im Fenster mit den Einstellungen für Kaspersky Security Center Web Console die Standard-Portnummern ändern.

   Neben den Ports 3333, 4004 und 4444 verwendet Kaspersky Security Center Web Console auch die Ports 4445, 2444 und 2445 für unterschiedliche Zwecke.

2. **Installieren der Identitäts- und Zugriffsverwaltung**

   Geben Sie während der Installation von Kaspersky Security Center Web Console an, dass Sie die Identitäts- und Zugriffsverwaltung installieren möchten. Wenn Sie dies nicht getan haben, führen Sie den Installationsassistenten der Kaspersky Security Center Web Console erneut aus.

3. **Konfigurieren der Identitäts- und Zugriffsverwaltung**

   Stellen Sie sicher, dass im Fenster mit den Einstellungen für Kaspersky Security Center Web Console der Umschalter **Identitäts- und Zugriffsverwaltung (IAM)** aktiviert ist. Geben Sie außerdem den DNS-Namen des Geräts mit installierter Kaspersky Security Center Web Console an: Die Client-Programme werden sich mit dem Gerät verbinden.

4. **Angeben der Token-Einstellungen**

   Geben Sie In dem Fenster mit den Einstellungen für Kaspersky Security Center Web Console die Lebensdauer der Token und das Timeout für die Autorisierung an, die von der Identitäts- und Zugriffsverwaltung verwendet werden. Sie können die Standardwerte verwenden oder entsprechend Ihren Anforderungen Ihre eigenen Werte angeben.

5. **Erteilen von Zertifikaten**

   Wenn Sie der Verwendung von Zertifikaten, die durch den Administrationsserver generiert wurden, bevorzugen, laden Sie im Einstellungsfenster von Kaspersky Security Center Web Console die Root-Zertifikate für die Ports herunter, die von IAM verwendet werden. Verteilen Sie diese anschließend auf den Workstations der Benutzer von Kaspersky Security Center Web Console. Andernfalls zeigen die Browser der Benutzer Fehlermeldungen an, wenn diese versuchen, eine Verbindung zur Kaspersky Security Center Web Console herzustellen.

6. **Registrieren der Server und Web-Oberflächen von Kaspersky Industrial CyberSecurity for Networks**

   Wenn IAM installiert ist, zeigt die Kaspersky Security Center Web Console eine Meldung an, dass ein oder mehrerer Server oder Web-Oberflächen von Kaspersky Industrial CyberSecurity for Networks auf die Registrierung warten. Klicken Sie auf diese Meldung, um Ihre Instanzen von Servern und Web-Oberflächen von Kaspersky Industrial CyberSecurity for Networks zu registrieren.

Ergebnisse

Nachdem Sie dieses Szenario abgeschlossen haben, können Sie für Kaspersky Industrial CyberSecurity for Networks und für die Kaspersky Security Center Web Console SSO und IAM verwenden.

Die Identitäts- und Zugriffsverwaltung in der Kaspersky Security Center Web Console konfigurieren

So konfigurieren Sie Identitäts- und Zugriffsverwaltung gemäß Ihren Anforderungen:

1. Wechseln Sie im Hauptmenü zu **Einstellungen** → **Identitäts- und Zugriffsverwaltung**.
2. Stellen Sie im Abschnitt **Identitäts- und Zugriffsverwaltung** sicher, dass die Identitäts- und Zugriffsverwaltung aktiviert ist.
3. Klicken Sie unterhalb der Zeile **Netzwerkname des Geräts mit installierter Identitäts- und Zugriffsverwaltung** auf den Link **Einstellungen**.
4. Geben Sie den DNS-Namen des Geräts an, auf dem Sie die Identitäts- und Zugriffsverwaltung installiert haben. Die Client-Programme werden eine Verbindung zu diesem Gerät herstellen.
5. Bei Bedarf können Sie die standardmäßigen Token-Einstellungen, die Zertifikatseinstellungen und die Portnummern durch Anklicken des Links **Einstellungen** unterhalb der entsprechenden Einstellungsgruppe ändern.

Die Identitäts- und Zugriffsverwaltung ist aktiviert und funktioniert gemäß Ihren Anforderungen.

Die Kaspersky Industrial CyberSecurity for Networks in der Kaspersky Security Center Web Console registrieren

Um mit der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks über die Kaspersky Security Center Web Console zu arbeiten, müssen Sie die Web-Oberfläche zunächst in der Web Console von Kaspersky Security Center registrieren.

So registrieren Sie die Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks:

1. Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:
   - Sie haben das Web-Plug-in von Kaspersky Industrial CyberSecurity for Networks heruntergeladen und installiert.

     Sie können dies jedoch auch später tun, während Sie auf die Synchronisation des Servers von Kaspersky Industrial CyberSecurity for Networks mit dem Administrationsserver warten.
   - Sie haben das Scenario for Single Sign-On (SSO) technology usage preparations abgeschlossen.
   - Die erforderlichen Einstellungen in der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks werden in Kaspersky Security Center festgelegt. Weitere Informationen finden Sie in der Online-Hilfe von Kaspersky Industrial CyberSecurity for Networks.
   - Sie sind mit einem Administratorkonto in der Kaspersky Security Center Web Console angemeldet.
   - IAM wurde konfiguriert.

2. Verschieben Sie das Gerät mit dem installierten Server von Kaspersky Industrial CyberSecurity for Networks von Gruppe "Nicht zugeordnete Geräte" in die Gruppe "Verwaltete Geräte":

   a. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Nicht zugeordnete Geräte**.

   b. Aktivieren Sie das Kontrollkästchen neben dem Gerät mit dem installierten Server von Kaspersky Industrial CyberSecurity for Networks.

   c. Klicken Sie auf die Schaltfläche **In Gruppe verschieben**.

   d. Aktivieren Sie in der Hierarchie der Administrationsgruppen das Kontrollkästchen neben der Gruppe "Verwaltete Geräte".

   e. Klicken Sie auf die Schaltfläche **Verschieben**.

3. Wechseln Sie zu den Eigenschaften des Geräts mit dem installierten Server von Kaspersky Industrial CyberSecurity for Networks.

4. Wählen Sie in den Geräteeigenschaften, im Abschnitt **Allgemein**, die Option **Verbindung zum Administrationsserver nicht trennen** aus und klicken Sie anschließend auf die Schaltfläche **Speichern**.

5. Wählen Sie im Eigenschaftenfenster des Geräts den Abschnitt **Programme** aus.

6. Wählen Sie im Abschnitt **Programme** die Option "Kaspersky Administrationsagent" aus.

7. Wenn der aktuelle Status des Geräts auf *Angehalten* steht, warten Sie, bis dieser auf *Gestartet* wechselt.

   Das kann bis zu 15 Minuten dauern. Wenn Sie das Web-Plug-in für Kaspersky Industrial CyberSecurity for Networks noch nicht installiert haben, können Sie dies jetzt tun, während Sie warten.

8. Wechseln Sie im Hauptmenü zu **Einstellungen → Identitäts- und Zugriffsverwaltung**.

   Im Feld **Registrierungsanfragen** wird eine ausstehende Anfrage angezeigt.

9. Klicken Sie unterhalb des Feldes **Registrierungsanfragen** auf den Link **Einstellungen**.

10. Aktivieren Sie in der sich öffnenden Liste der registrierten Clients das Kontrollkästchen neben dem Namen des Servers von Kaspersky Industrial CyberSecurity for Networks mit dem Status *Ausstehend* und klicken Sie anschließend auf die Schaltfläche **Genehmigen**.

    Wenn Sie den Server von Kaspersky Industrial CyberSecurity for Networks nicht registrieren möchten, können Sie auf die Schaltfläche "Ablehnen" klicken und später zu dieser Liste zurückkehren.

    Nachdem Sie auf die Schaltfläche **Genehmigen** geklickt haben, ändert sich der Status auf *Genehmigt* und anschließend auf *Bereit*. Wenn sich der Status nicht ändert, können Sie auf die Schaltfläche "Aktualisieren" klicken.

11. Schließen Sie die Liste der registrierten Clients und stellen Sie sicher, dass sich der Wert Feld **Registrierte Clients** erhöht hat.

12. So fügen Sie das Widget von Kaspersky Industrial CyberSecurity for Networks zum Dashboard hinzu:

    a. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Dashboard**.

    b. Klicken Sie im Dashboard auf die Schaltfläche **Web-Widget hinzufügen oder wiederherstellen**.

    c. Wählen Sie im sich öffnenden Widget-Menü die Option **Andere**.

    d. Wählen Sie das Widget von Kaspersky Industrial CyberSecurity for Networks aus.

Sie können jetzt über den Link im Widget zur Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks wechseln.

Nachdem Sie den Registrierungsvorgang abgeschlossen haben, wird eine neue Schaltfläche namens **Kaspersky Security Center** auf der Anmeldeseite der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks angezeigt. Sie können auf diese Schaltfläche klicken, um sich mit Ihren Zugangsdaten für Kaspersky Security Center an der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks anzumelden.

Token-Lebensdauer und Autorisierungs-Timeout der Identitäts- und Zugriffsverwaltung

Beim Konfigurieren der Identitäts- und Zugriffsverwaltung (auch als IAM bezeichnet) müssen Sie die Einstellungen für die Lebensdauer der Token und das Timeout der Autorisierungen angeben. Die Standardeinstellungen sind so konzipiert, dass sie sowohl die Sicherheitsstandards als auch die Serverlast berücksichtigen. Sie können diese Einstellungen jedoch gemäß den Richtlinien Ihrer Organisation ändern.

Wenn ein Token abläuft, stellt IAM diesen automatisch erneut aus.

In der folgenden Tabelle sind die Standardeinstellungen für die Token-Lebensdauer aufgeführt.

Einstellungen der Token-Lebensdauer

Token	Standardlebensdauer (in Sekunden)	Beschreibung
Identitätstoken (id_token)	86400	Identitätstoken, das vom OAuth 2.0-Client verwendet wird (d. h. entweder Kaspersky Security Center Web Console oder Kaspersky Industrial CyberSecurity Console). IAM sendet ID-Token, die Informationen über den Benutzer enthalten (d. h. das Benutzerprofil) an den Client.
Zugriffstoken (access_token)	86400	Zugriffstoken, der vom OAuth 2.0-Client verwendet wird, um im Namen des von IAM identifizierten Ressourcenbesitzers auf den Ressourcenserver zuzugreifen.
Aktualisierungstoken (refresh_token)	172800	Der OAuth 2.0-Client verwendet diesen Token zum erneuten Ausstellen des Identitätstokens und des Zugriffstokens.

In der folgenden Tabelle sind die Timeouts für "auth_code" und "login_consent_request" aufgeführt.

Einstellungen des Autorisierungs-Timeouts

Einstellung	Standard-Timeout (in Sekunden)	Beschreibung
Autorisierungscode (auth_code)	3600	Timeout für das Austauschen von Code des Tokens. Der OAuth 2.0-Client sendet diesen Code an den Ressourcenserver und erhält im Gegenzug den Zugriffstoken.
Zeitüberschreitung von Login- und Übereinstimmungsanfragen (login_consent_request)	3600	Timeout für das Delegieren von Benutzerrechten an den OAuth 2.0-Client.

Weitere Informationen zu Token finden Sie auf der Website von OAuth.

So konfigurieren Sie den Timeout für Clients, für die keine Maus- oder Tastaturaktivität erkannt wurde:

1. Öffnen Sie im Installationsordner der Kaspersky Security Center Web Console die Datei "config.json". Die Datei enthält die Parameter zur Konfiguration der Timeouts für inaktive Clients.

2. Verwenden Sie den Parameter `clientIdleTimeout`, um die Zeit in Millisekunden anzugeben, nach deren Ablauf ein inaktiver Client eine Pop-up-Warnung anzeigt.

3. Verwenden Sie den Parameter `clientLogoutTimeout`, um die Zeit in Millisekunden anzugeben, nach deren Ablauf die IAM-Autorisierung für den inaktiven Client beendet wird. Der `clientLogoutTimeout` zählt nach Eintreten des `clientIdleTimeout` sequentiell rückwärts.

IAM-Zertifikate herunterladen und verteilen

Standardmäßig verwendet die Identitäts- und Zugriffsverwaltung die vom Administrationsserver generierten Zertifikate, um Browsern den Zugriff auf die Kaspersky Security Center Web Console zu gewähren. Bei Bedarf können Sie jedoch benutzerdefinierte Zertifikate verwenden. Unabhängig davon, welches Zertifikat Sie verwenden, müssen Sie sicherstellen, dass alle Workstations, von denen aus Benutzer von Kaspersky Security Center Web Console auf die Kaspersky Security Center Web Console zugreifen, diesem Zertifikat vertrauen.

So laden Sie Zertifikate herunter und verteilen sie:

1. Wechseln Sie im Hauptmenü zu **Einstellungen** → **Identitäts- und Zugriffsverwaltung**.

2. Klicken Sie für jedes Zertifikat auf den Link **Einstellungen** unter der entsprechenden Einstellungsgruppe und führen Sie dann einen der folgenden Schritte aus:

   - Wenn Sie das Zertifikat verwenden möchten, das der Administrationsserver bei der Installation von Kaspersky Security Center Web Console erstellt hat:

     1. Wählen Sie im sich öffnenden Fenster mit den Zertifikatseigenschaften die Option **Vom Administrationsserver generiert** aus.

     2. Klicken Sie auf **Download**, um das Zertifikat herunterzuladen.

     3. Verteilen Sie das heruntergeladene Zertifikat an alle Workstations, von denen die Benutzer von Kaspersky Security Center Web Console auf die Kaspersky Security Center Web Console zugreifen.

   - Wenn Sie ein Zertifikat besitzen, das Sie verwenden möchten:

     1. Wählen Sie im sich öffnenden Fenster mit den Zertifikatseigenschaften die Option **Benutzerdefiniertes TLS-Zertifikat** aus.

     2. Wählen Sie die Zertifikatsdatei und den privaten Schlüssel aus.

     3. Klicken Sie auf die Schaltfläche **OK**.

     4. Verteilen Sie das Zertifikat an alle Workstations, von denen aus Benutzer auf die Kaspersky Security Center Web Console oder die Kaspersky Industrial CyberSecurity Console zugreifen.

Die Zertifikate gewähren den Benutzern Zugriff auf die Kaspersky Security Center Web Console und die Kaspersky Industrial CyberSecurity Console.

Sie müssen alle Zertifikate zeitnah erneut ausstellen. Die vom Administrationsserver generierten Zertifikate müssen manuell erneut generiert werden. Die vom Installer der Kaspersky Security Center Web Console generierten Zertifikate müssen mittels Installer erneut generiert werden.

Die Identitäts- und Zugriffsverwaltung deaktivieren

Bei Bedarf können Sie die Identitäts- und Zugriffsverwaltung (auch als IAM bezeichnet) deaktivieren.

So deaktivieren Sie IAM:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Integration**.
2. Deaktivieren Sie im Abschnitt **Identitäts- und Zugriffsverwaltung** den Umschalter **Identitäts- und Zugriffsverwaltung**.

Sie können IAM später jederzeit aktivieren.

Wenn Sie Kaspersky Security Center Web Console über das Installationsprogramm aktualisieren und angeben, dass Sie IAM nicht installieren möchten, wird Kaspersky Security Center Web Console aktualisiert und IAM wird nicht installiert. Alle Informationen über die Integration mit Kaspersky Industrial CyberSecurity for Networks werden mitsamt den IAM-Konfigurationsdateien und Protokolldateien von Ihrem Gerät gelöscht.

Domänenauthentifizierung mithilfe der Protokolle NTLM und Kerberos konfigurieren

Mit Kaspersky Security Center 15.1 können Sie die Domänenauthentifizierung in OpenAPI mithilfe der Protokolle NTLM und Kerberos verwenden. Ein Windows-Benutzer, der die Domänenauthentifizierung verwendet, kann die sichere Authentifizierung in Kaspersky Security Center Web Console aktivieren, ohne das Kennwort im Unternehmensnetzwerk erneut eingeben zu müssen (Single Sign-on).

Die Domänenauthentifizierung in OpenAPI über das Kerberos-Protokoll hat folgende Einschränkungen:

- Der Benutzer von Kaspersky Security Center Web Console muss in Active Directory mithilfe des Kerberos-Protokolls authentifiziert werden. Der Benutzer muss ein gültiges Kerberos Ticket Granting Ticket (auch TGT genannt) haben. Ein TGT wird automatisch ausgestellt, wenn Sie sich bei der Domäne authentifizieren.
- Sie müssen die Kerberos-Authentifizierung im Browser konfigurieren. Einzelheiten finden Sie in der Dokumentation Ihres Browsers.

Wenn Sie die Domänenauthentifizierung mithilfe von Kerberos-Protokollen verwenden möchten, muss Ihr Netzwerk die folgenden Bedingungen erfüllen:

- Der Administrationsserver muss unter dem Namen des Domänenkontos ausgeführt werden.
- Der Server der Web Console von Kaspersky Security Center muss auf demselben Gerät installiert werden, auf dem der Administrationsserver installiert ist.

- Sie müssen die folgenden Service Principal Names (SPN) für das Administrationsserver-Benutzerkonto angeben:

  - "http/<fqnd-Name.des.Servers>"

  - "http/<Server>"

  Dabei steht "<server>" für den Netzwerknamen des Geräts mit installiertem Administrationsserver und "<server.fqnd.name>" für den FQDN-Namen dieses Gerät.

- Bei einer Verbindung über die Verwaltungskonsole oder Kaspersky Security Center Web Console muss die Adresse des Administrationsservers genauso angegeben werden, wie die Adresse, für die der SPN (Service Principal Name) registriert ist. Sie können entweder <fqnd-Name.des.Servers> oder <Server> angeben.

- Für eine Anmeldung ohne Kennworteingabe muss der Browserprozess, in dem Kaspersky Security Center Web Console als Browser geöffnet ist, unter einem Domänenkonto ausgeführt werden.

Kerberos- und NTLM-Protokolle werden nur in OpenAPI für Kaspersky Security Center 15.1 unterstützt. In OpenAPI für Kaspersky Security Center Linux werden sie nicht unterstützt.

Konfigurieren des Administrationsservers

Dieser Abschnitt beschreibt den Konfigurationsprozess und die Eigenschaften des Kaspersky Security Center Administrationsservers.

Verbindung zwischen Kaspersky Security Center Web Console und Administrationsserver anpassen

So legen Sie die Verbindungsports des Administrationsservers fest:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verbindungsports** aus.

Die Anwendung zeigt die wichtigsten Verbindungseinstellungen des ausgewählten Servers an.

Die Kaspersky Security Center Web Console ist über den SSL-Port TCP 13299 mit dem Administrationsserver verbunden. Derselbe Port kann von klakaut-Automatisierungsobjekten verwendet werden.

Der Port TCP 14000 kann für die Verbindung der Kaspersky Security Center Web Console, der Verteilungspunkte, der sekundären Administrationsserver und der Automatisierungsobjekte des Tools klakaut sowie für das Abrufen der Daten von den Client-Geräten verwendet werden.

Der SSL-Port TCP 13000 kann normalerweise nur vom Administrationsagenten, einem sekundären Administrationsserver und dem primären Administrationsserver in der DMZ verwendet werden. In einigen Fällen kann eine Verbindung der Kaspersky Security Center Web Console über den SSL-Port 13000 erforderlich sein:

- Bei Verwendung desselben SSL-Ports sowohl für die Kaspersky Security Center Web Console als auch für andere Aktivitäten (Abrufen der Daten von den Client-Geräten, Verbindung mit Verteilungspunkten, Verbindung mit sekundären Administrationsservern).
- Wenn das Automatisierungsobjekt des Tools klakaut nicht direkt mit dem Administrationsserver, sondern über den Verteilungspunkt in der DMZ verbunden wird.

Protokollierung der Verbindungsereignisse des Administrationsservers konfigurieren

Der Verlauf der Verbindungen und Versuche, während des Betriebs eine Verbindung mit dem Administrationsserver herzustellen, können in einer Protokolldatei gespeichert werden. Mit den Informationen in der Datei können Sie nicht nur Verbindungen innerhalb Ihrer Netzwerkinfrastruktur verfolgen, sondern auch nicht autorisierte Versuche, auf den Server zuzugreifen.

So protokollieren Sie die Ereignisse der Verbindung zum Administrationsserver:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verbindungsports** aus.

3. Aktivieren Sie die Option **Verbindungsereignisse des Administrationsservers protokollieren**.

Alle weiteren Ereignisse eingehender Verbindungen zum Administrationsserver, Authentifizierungsergebnisse und SSL-Fehler werden in der Datei %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog gespeichert.

Die Internetzugriffseinstellungen für den Administrationsserver konfigurieren

Sie müssen den Internetzugang anpassen, um Kaspersky Security Network zu verwenden und um Updates für die Antiviren-Datenbanken von Kaspersky Security Center und die verwalteten Kaspersky-Anwendungen herunterzuladen.

So geben Sie die Internetzugriffseinstellungen für den Administrationsserver an:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Konfiguration des Internetzugriffs** aus.

3. Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

   - **Adresse**

     Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center mit dem Internet.

   - **Port**

     Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center hergestellt wird.

   - **Proxyserver für lokale Adressen umgehen**

     Bei der Verbindung mit den Geräten im lokalen Netzwerk wird kein Proxyserver verwendet.

   - **Authentifizierung am Proxyserver**

     Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

     Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver verwenden** aktiviert ist.

   - **Benutzername**

     Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

   - **Kennwort**

     Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

     Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

Sie können den Internetzugang auch unter Verwendung des Schnellstartassistenten konfigurieren.

Maximalen Anzahl an Ereignissen in der Ereignis-Datenverwaltung festlegen

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignis-Datenverwaltung** die Einstellungen für das Speichern der Ereignisse in der Administrationsserver-Datenbank anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Wenn Sie die maximale Anzahl der Ereignisse angeben, berechnet die Anwendung einen ungefähren Wert des für die angegebene Zahl benötigten Speicherplatzes. Sie können diese ungefähre Berechnung verwenden, um zu überprüfen, ob Sie ausreichen freien Platz auf dem Laufwerk haben, um einen Überlauf der Datenbank zu vermeiden. Standardmäßig umfasst die Administrationsserver-Datenbank 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Die Anwendung überprüft die Datenbank alle 10 Minuten. Wenn die Anzahl der Ereignisse den festgelegten Höchstwert plus 10.000 erreicht, löscht die Anwendung die ältesten Ereignisse, sodass nur noch die festgelegte Höchstanzahl von Ereignissen übrig bleibt.

Wenn der Administrationsserver alte Ereignisse löscht, kann er keine neuen Ereignisse in der Datenbank speichern. Während dieser Zeitspanne werden Informationen über abgelehnte Ereignisse in das Kaspersky-Ereignisprotokoll geschrieben. Die neuen Ereignisse werden in die Warteschlange verschoben und dann in der Datenbank gespeichert, nachdem der Löschvorgang abgeschlossen wurde.

Um die Anzahl der Ereignisse, die in der Ereignis-Datenverwaltung des Administrationsservers gespeichert werden können, zu begrenzen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Ereignis-Datenverwaltung** aus. Geben Sie die maximale Anzahl von Ereignissen an, die in der Datenbank gespeichert sind.

3. Klicken Sie auf die Schaltfläche **Speichern**.

Zusätzlich können Sie Folgendes tun:

- Die Einstellungen einer beliebigen Aufgabe ändern, um entweder Ereignisse im Zusammenhang mit dem Aufgabenfortschritt oder nur die Ergebnisse der Aufgabenausführung zu speichern.

- Die Speicherdauer verkürzen oder deaktivieren für Ereignisse des Administrationsservers, des Administrationsagenten und der Kaspersky-Anwendungen, die auf den verwalteten Geräten installiert sind.

Auf diese Weise reduzieren Sie die Anzahl der Ereignisse in der Datenbank, erhöhen die Ausführungsgeschwindigkeit der Szenarien, die mit der Analyse der Ereignistabelle in der Datenbank verbunden sind, und reduzieren das Risiko der Verdrängung von kritischen Ereignissen durch eine große Anzahl an Ereignissen.

Verbindungseinstellungen des Geräts mit Schutz auf UEFI-Ebene

Ein *Gerät mit Schutz auf UEFI-Ebene* ist ein Gerät mit einer Lösung oder Anwendung von Kaspersky, die auf BIOS-Ebene integriert ist. Der integrierte Schutz gewährleistet die Sicherheit des Geräts bereits ab Beginn des Systemstarts, während der Schutz für Geräte, die keine integrierte Software haben, erst nach dem Start der Sicherheitsanwendung in Aktion tritt. Kaspersky Security Center unterstützt die Verwaltung von solchen Geräten.

Um die Einstellungen der Verbindung von Geräten mit Schutz auf UEFI-Ebene zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Zusätzliche Ports** aus.

3. Ändern Sie die entsprechenden Einstellungen:

   - **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS öffnen**

     Geräte mit Schutz auf UEFI-Ebene können eine Verbindung mit dem Administrationsserver herstellen.

- **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS**

  Sie können die Portnummer ändern, wenn die Option **Port für Geräte mit Schutz auf UEFI-Ebene und Geräte mit KasperskyOS öffnen** aktiviert ist. Standardmäßig wird Portnummer 13294 verwendet.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Geräte mit Schutz auf UEFI-Ebene können jetzt eine Verbindung mit dem Administrationsserver herstellen.

Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen

Sekundären Administrationsserver hinzufügen (Ausführung auf dem zukünftigen primären Administrationsserver)

Sie können einen Administrationsserver als sekundären Administrationsserver hinzufügen und so eine Hierarchie vom Typ "primärer/sekundärer" festlegen.

Um einen sekundären Administrationsserver hinzuzufügen, der mit Kaspersky Security Center Web Console verbunden werden kann, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Port 13000 des zukünftigen primären Administrationsservers für die Annahme von Verbindungen von sekundären Administrationsservern verfügbar ist.
2. Klicken Sie auf dem zukünftigen primären Administrationsserver auf das Einstellungen-Symbol ( ).
3. Wählen Sie auf der folgenden Eigenschaftenseite auf die Registerkarte **Administrationsserver**.
4. Wählen Sie das Kontrollkästchen neben der Administrationsgruppe aus, zu der Sie den virtuellen Administrationsserver hinzufügen möchten.
5. Klicken Sie in der Menüleiste auf **Sekundären Administrationsserver verbinden**.

   Der Assistent für das Hinzufügen eines sekundären Administrationsservers wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
6. Füllen Sie die folgenden Felder aus:

   - **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**

     Wählen Sie diese Option, wenn sich der sekundäre Administrationsserver in einer demilitarisierten Zone (DMZ) befindet.

     Wenn diese Option aktiviert ist, müssen Sie die Parameter der **Adresse des sekundären Servers** angeben.

     Wenn diese Option ausgewählt ist, initiiert der primäre Administrationsserver die Verbindung mit dem sekundären Administrationsserver. Andernfalls verbindet sich der sekundäre Administrationsserver mit dem primären Administrationsserver.

   - **Anzeigename des sekundären Administrationsservers**

     Ein Name, unter dem der sekundäre Administrationsserver in der Hierarchie angezeigt werden soll. Wenn Sie möchten, können Sie als Name die IP-Adresse oder einen Benutzernamen wie "Sekundärer Server für Gruppe 1" angeben.

- **Adresse des sekundären Administrationsservers (optional)**

  Geben Sie die IP-Adresse oder den Domänennamen des sekundären Administrationsservers an.

  Dieser Parameter ist erforderlich, wenn die Option **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden** aktiviert ist.

- **SSL-Port des Administrationsservers**

  Geben Sie die Nummer des SSL-Ports auf dem primären Administrationsserver an. Standardmäßig wird Portnummer 13000 verwendet.

- **API-Port des Administrationsservers**

  Geben Sie die Nummer des Ports auf dem primären Aministrationsserver an, über den Verbindungen über OpenAPI eingehen sollen. Standardmäßig wird Portnummer 13299 verwendet.

7. Geben Sie das Zertifikat für den sekundären Administrationsserver an. Wenn Sie den Parameter **Adresse des sekundären Servers** angegeben haben, können Sie auf **Vom sekundären Administrationsserver abrufen** klicken, um das Zertifikat auf diese Weise zu erhalten. Klicken Sie andernfalls auf die Schaltfläche **Zertifikatsdatei auswählen** und geben Sie den Pfad zur Zertifikatsdatei an.

8. Legen Sie die Verbindungseinstellungen fest:

   - Geben Sie die Adresse des zukünftigen primären Administrationsservers ein.

   - Wenn der zukünftige sekundäre Administrationsserver einen Proxyserver verwendet, geben Sie die Adresse des Proxyservers und die Anmeldeinformationen des Benutzers ein, um sich mit dem Proxyserver zu verbinden.

9. Geben Sie die Zugangsdaten des Benutzers ein, der Zugriffsrechte auf den zukünftigen sekundären Administrationsserver hat.

10. Wenn die zweistufige Überprüfung aktiviert und konfiguriert ist, geben Sie den Sicherheitscode an, der von der Authenticator-App generiert wurde.

    Wenn die zweistufige Überprüfung für das von Ihnen angegebene Konto aktiviert, aber nicht konfiguriert, ist, erstellen Sie die Hierarchie vom zukünftigen sekundären Server (siehe Anweisungen unten).

Wenn die Verbindungseinstellungen korrekt sind, wird die Verbindung mit dem zukünftigen sekundären Server hergestellt und die "primär/sekundär"-Hierarchie gebildet. Wenn die Verbindung fehlgeschlagen ist, überprüfen Sie die Verbindungseinstellungen oder geben Sie das Zertifikat des zukünftigen sekundären Servers manuell an.

Die Verbindung zwischen dem primären und dem sekundären Administrationsserver wird über Port 13000 hergestellt. Die vom primären Administrationsserver bereitgestellten Aufgaben und Richtlinien werden abgerufen und angewendet. Der sekundäre Administrationsserver wird auf dem primären Administrationsserver in der Administrationsgruppe angezeigt, in der er hinzugefügt wurde.

Sekundären Administrationsserver hinzufügen (Ausführung auf dem zukünftigen sekundären Administrationsserver)

Wenn Sie keine Verbindung zum zukünftigen sekundären Administrationsserver aufbauen konnten (da dieser z. B. vorübergehend getrennt oder nicht verfügbar war), können Sie trotzdem einen sekundären Administrationsserver hinzufügen.

Um einen Administrationsserver, der nicht für die Verbindung über Kaspersky Security Center Web Console verfügbar ist, als sekundären Server hinzuzufügen, gehen Sie wie folgt vor:

1. Senden Sie die Zertifikatsdatei des zukünftigen primären Administrationsservers an den Systemadministrator des Büros, in dem sich der zukünftige sekundäre Administrationsserver befindet (Sie können die Datei z. B. auf einem externen Gerät wie einem Flash-Laufwerk speichern oder per E-Mail senden).

   Die Zertifikatsdatei befindet sich auf dem zukünftigen primären Administrationsserver unter %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Bitten Sie den Systemadministrator, der für den zukünftigen sekundären Administrationsserver zuständig ist, wie folgt vorzugehen:

   a. Klicken Sie auf das Einstellungen-Symbol ( ).

   b. Wechseln Sie auf der nächsten Seite mit Eigenschaften zum Abschnitt **Hierarchie der Administrationsserver** auf der Registerkarte **Allgemein**.

   c. Wählen Sie die Option **Dieser Administrationsserver ist in der Server-Hierarchie sekundär** aus.

   d. Geben Sie im Feld **Adresse des primären Administrationsservers** den Netzwerknamen des zukünftigen primären Administrationsservers an.

   e. Wählen Sie die zuvor gespeicherte Zertifikatsdatei des zukünftigen primären Administrationsservers aus, indem Sie auf **Durchsuchen** klicken.

   f. Aktivieren Sie bei Bedarf das Kontrollkästchen **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**.

   g. Wenn die Verbindung mit dem zukünftigen sekundären Administrationsserver über einen Proxyserver hergestellt wird, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie die Verbindungseinstellungen ein.

   h. Klicken Sie auf die Schaltfläche **Speichern**.

Die "primär/sekundär"-Hierarchie wird gebildet. Der primäre Administrationsserver nimmt über Port 13000 Verbindungen vom sekundären Administrationsserver an. Die vom primären Administrationsserver bereitgestellten Aufgaben und Richtlinien werden abgerufen und angewendet. Der sekundäre Administrationsserver wird auf dem primären Administrationsserver in der Administrationsgruppe angezeigt, in der er hinzugefügt wurde.

Liste mit sekundären Administrationsservern anzeigen

So zeigen Sie eine Liste mit sekundären (einschl. virtuellen) Administrationsservern an:

Klicken Sie im Hauptmenü auf den Namen des Administrationsservers neben dem Einstellungen-Symbol ( ).

Eine Dropdown-Liste mit sekundären (einschl. virtuellen) Administrationsservern wird angezeigt.

Sie können auf den Namen eines dieser Administrationsserver klicken, um zu ihm zu wechseln.

Die Administrationsgruppen werden ebenfalls angezeigt, sind jedoch ausgegraut und stehen in diesem Menü nicht zur Verwaltung zur Verfügung.

Wenn Sie in der Kaspersky Security Center Web Console mit Ihrem primären Administrationsserver verbunden sind und keine Verbindung zu einem virtuellen Administrationsserver, der von einem sekundären Administrationsserver verwaltet wird, herstellen können, haben Sie folgende Möglichkeiten:

- **Ändern Sie die vorhandene Installation von Kaspersky Security Center Web Console, um den sekundären Server zur Liste der vertrauenswürdigen Administrationsserver hinzuzufügen.** Anschließend können Sie sich in Kaspersky Security Center Web Console mit dem virtuellen Administrationsserver verbinden.

  1. Führen Sie auf dem Gerät, auf dem Kaspersky Security Center Web Console installiert ist, die ausführbare Datei ksc-web-console.<Versionsnummer>.<Build-Nummer>.exe unter einem Benutzerkonto mit Administratorrechten aus.

     Der Installationsassistent wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

  2. Wählen Sie die Option **Aktualisieren** aus.

  3. Wählen Sie im Schritt **Änderungstyp** die Option **Verbindungseinstellungen ändern** aus.

  4. Fügen Sie im Schritt **Vertrauenswürdige Administrationsserver** den erforderlichen sekundären Administrationsserver hinzu.

  5. Klicken Sie im letzten Schritt auf **Ändern**, um die neuen Einstellungen zu übernehmen.

  6. Nach dem erfolgreichen Abschluss der Neukonfigurierung der Anwendung klicken Sie auf die Schaltfläche **Fertigstellen**.

- Verwenden Sie die Kaspersky Security Center Web Console, um eine direkte Verbindung mit dem sekundären Administrationsserver herzustellen auf dem der virtuelle Server erstellt wurde. Anschließend können Sie in Kaspersky Security Center Web Console zum virtuellen Administrationsserver wechseln.

- Verwenden Sie die MMC-basierte Verwaltungskonsole zum Herstellen einer direkten Verbindung mit dem virtuellen Server.

Administrationsserver-Hierarchie löschen

Wenn Sie keine Hierarchie von Administrationsservern mehr verwenden möchten, können Sie diese von dieser Hierarchie trennen.

So löschen Sie eine Hierarchie von Administrationsservern:

1. Klicken Sie im Hauptmenü neben dem Namen des primären Administrationsservers auf das Einstellungen-Symbol ( ).

2. Gehen Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.

3. Wählen Sie in der Administrationsgruppe, aus der Sie den sekundären Administrationsserver löschen möchten, den entsprechenden Server aus.

4. Klicken Sie in der Menüleiste auf **Löschen**.

5. Klicken Sie im nächsten Fenster auf **OK**, um das Löschen des sekundären Administrationsservers zu bestätigen.

Der ehemalige primäre Administrationsserver und der ehemalige sekundäre Administrationsserver sind nun unabhängig voneinander. Die Hierarchie ist nicht mehr vorhanden.

Wartung des Administrationsservers

Die Wartung des Administrationsservers ermöglicht die Freigabe von Speicherplatz im Ordner des Administrationsservers und das Reduzieren der Datenbankgröße, indem nicht mehr benötigte Objekte gelöscht werden. Dies trägt zu einer verbesserten Leistung und erhöhten Ausführungszuverlässigkeit der Anwendung bei. Es wird empfohlen, den Administrationsserver mindestens einmal pro Woche zu warten.

Die Wartung des Administrationsservers erfolgt mithilfe der entsprechenden Aufgaben. Bei der Wartung des Administrationsservers führt das Programm die folgenden Aktionen aus:

- Es werden nicht benötigte Ordner und Dateien aus dem Ablageordner gelöscht.
- Es werden nicht benötigte Datensätze aus Tabellen gelöscht (auch als "hängender Zeiger" bekannt).
- Es wird der Cache geleert.
- Es wird die Datenbank gewartet (bei Verwendung von SQL Server oder PostgreSQL als DBMS):
  - Die Datenbank wird auf Fehler geprüft (nur SQL Server).
  - Die Datenbanken wird neu indiziert.
  - Die Datenbankstatistik wird aktualisiert.
  - Datenbank komprimieren (falls erforderlich).

Die Aufgabe Wartung des Administrationsservers wird bei der Installation von Kaspersky Security Center automatisch erstellt. Falls die Aufgabe Wartung des Administrationsservers gelöscht wurde, können Sie diese manuell erstellen.

So erstellen Sie die Aufgabe Wartung des Administrationsservers:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.

3. Wählen Sie im Fenster **Einstellungen der neue Aufgabe** des Assistenten den Aufgabentyp **Wartung des Administrationsservers** und klicken Sie auf die Schaltfläche **Weiter**.

4. Folgen Sie den weiteren Schritten des Assistenten.

Daraufhin wird die neu erstellte Aufgabe in der Aufgabenliste angezeigt. Für einen Administrationsserver kann nur eine Aufgabe des Typs Wartung des Administrationsservers ausgeführt werden. Wenn für den Administrationsserver bereits eine Aufgabe des Typs Wartung des Administrationsservers erstellt wurde, ist es nicht möglich, eine weitere Aufgabe des Typs Wartung des Administrationsservers zu erstellen.

Schnittstelle konfigurieren

Sie können die Benutzeroberfläche der Kaspersky Security Center Web Console so konfigurieren, dass Abschnitte und Elemente der Benutzeroberfläche abhängig von den verwendeten Funktionen ein- und ausgeblendet werden.

So konfigurieren Sie die Benutzeroberfläche der Kaspersky Security Center Web Console gemäß den derzeit verwendeten Funktionen:

1. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Einstellungen der Benutzeroberfläche.**
2. Aktivieren oder deaktivieren Sie im folgenden Fenster **Einstellungen der Benutzeroberfläche** die erforderlichen Optionen.
3. Klicken Sie auf **Speichern**.

   Danach werden die Abschnitte des Hauptmenüs in der Konsole entsprechend den aktivierten Optionen angezeigt. Wenn Sie beispielsweise **Alarme von EDR anzeigen** aktivieren, wird der Abschnitt **Überwachung und Berichterstattung** → **Alarme** im Hauptmenü angezeigt.

Virtuelle Administrationsserver verwalten

Dieser Abschnitt beschreibt die folgenden Vorgänge für die Verwaltung von virtuellen Administrationsservern:

- Virtuelle Administrationsserver erstellen
- Virtuelle Administrationsserver aktivieren und deaktivieren
- Virtuellen Administrationsservern einen Administrator zuweisen
- Den Administrationsserver für Client-Geräte wechseln
- Virtuelle Administrationsserver löschen

Einen virtuellen Administrationsserver erstellen

Sie können virtuelle Administrationsserver erstellen und sie zu Administrationsgruppen hinzufügen.

Wenn Sie einen virtuellen Administrationsserver erstellen, erbt dieser die Benutzerliste und alle Benutzerrechte des primären Administrationsservers. Wenn ein Benutzer Zugriffsrechte auf den primären Server besitzt, hat dieser Benutzer auch Zugriffsrechte auf den virtuellen Server. Nach der Erstellung konfigurieren Sie die Zugriffsrechte auf die Server unabhängig.

Um einen virtuellen Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

2. Gehen Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.

3. Wählen Sie die Administrationsgruppe aus, zu der Sie den virtuellen Administrationsserver hinzufügen möchten. Der virtuelle Administrationsserver wird die Geräte dieser ausgewählten Gruppe (einschließlich der Untergruppen) verwalten.

4. Klicken Sie in der Menüleiste auf **Neuer virtueller Administrationsserver**.

5. Legen Sie auf der nächsten Seite die Eigenschaften des neuen virtuellen Administrationsservers fest:

   - **Name des virtuellen Administrationsservers**.

   - **Verbindungsadresse des Administrationsservers**

     Sie können den Namen oder die IP-Adresse Ihres Administrationsservers angeben.

6. Wählen Sie aus der Benutzerliste den Administrator des virtuellen Administrationsservers aus. Bei Bedarf können Sie vor der Zuweisung der Administratorrolle eines der vorhandenen Benutzerkonten bearbeiten oder ein neues Benutzerkonto erstellen.

7. Klicken Sie auf die Schaltfläche **Speichern**.

Der neue virtuelle Administrationsserver wird erstellt, zur Administrationsgruppe hinzugefügt und auf der Registerkarte **Administrationsserver** angezeigt.

Wenn Sie in der Kaspersky Security Center Web Console mit Ihrem primären Administrationsserver verbunden sind und keine Verbindung zu einem virtuellen Administrationsserver, der von einem sekundären Administrationsserver verwaltet wird, herstellen können, haben Sie folgende Möglichkeiten:

- **Ändern Sie die vorhandene Installation von Kaspersky Security Center Web Console, um den sekundären Server zur Liste der vertrauenswürdigen Administrationsserver hinzuzufügen.** Anschließend können Sie sich in Kaspersky Security Center Web Console mit dem virtuellen Administrationsserver verbinden.

  1. Führen Sie auf dem Gerät, auf dem Kaspersky Security Center Web Console installiert ist, die ausführbare Datei ksc-web-console.<Versionsnummer>.<Build-Nummer>.exe unter einem Benutzerkonto mit Administratorrechten aus.

     Der Installationsassistent wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

  2. Wählen Sie die Option **Aktualisieren** aus.

  3. Wählen Sie im Schritt **Änderungstyp** die Option **Verbindungseinstellungen ändern** aus.

  4. Fügen Sie im Schritt **Vertrauenswürdige Administrationsserver** den erforderlichen sekundären Administrationsserver hinzu.

  5. Klicken Sie im letzten Schritt auf **Ändern**, um die neuen Einstellungen zu übernehmen.

  6. Nach dem erfolgreichen Abschluss der Neukonfigurierung der Anwendung klicken Sie auf die Schaltfläche **Fertigstellen**.

- Verwenden Sie die Kaspersky Security Center Web Console, um eine direkte Verbindung mit dem sekundären Administrationsserver herzustellen auf dem der virtuelle Server erstellt wurde. Anschließend können Sie in Kaspersky Security Center Web Console zum virtuellen Administrationsserver wechseln.

- Verwenden Sie die MMC-basierte Verwaltungskonsole zum Herstellen einer direkten Verbindung mit dem virtuellen Server.

Einen virtuellen Administrationsserver aktivieren und deaktivieren

Wenn Sie einen neuen virtuellen Administrationsserver erstellen, ist dieser standardmäßig aktiviert. Sie können ihn jederzeit aktivieren oder deaktivieren. Das Aktivieren oder Deaktivieren eines virtuellen Administrationsservers kommt dem Ein- und Ausschalten eines physischen Administrationsservers gleich.

So aktivieren oder deaktivieren Sie einen virtuellen Administrationsserver:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.

3. Wählen Sie den virtuellen Administrationsserver aus, den Sie aktivieren oder deaktivieren möchten.

4. Klicken Sie auf der Menüleiste auf die Schaltfläche **Virtuellen Administrationsserver aktivieren / deaktivieren**.

Der Status des virtuellen Administrationsservers ändert sich abhängig vom vorherigen Status in "Aktiviert" oder "Deaktiviert". Der aktualisierte Status wird neben dem Namen des Administrationsservers angezeigt.

Einem virtuellen Administrationsserver einen Administrator zuweisen

Wenn Sie in Ihrem Unternehmen virtuelle Administrationsserver verwenden, möchten Sie möglicherweise jedem virtuellen Administrationsserver einen eigenen Administrator zuweisen. Dies kann beispielsweise nützlich sein, wenn Sie virtuelle Administrationsserver erstellen, um separate Büros oder Abteilungen Ihrer Organisation zu verwalten, oder wenn Sie ein MSP-Anbieter sind und Sie Ihre Mandanten über virtuelle Administrationsserver verwalten möchten.

Wenn Sie einen virtuellen Administrationsserver erstellen, erbt dieser die Benutzerliste und alle Benutzerrechte des primären Administrationsservers. Wenn ein Benutzer Zugriffsrechte auf den primären Server besitzt, hat dieser Benutzer auch Zugriffsrechte auf den virtuellen Server. Nach der Erstellung konfigurieren Sie die Zugriffsrechte auf die Server unabhängig. Wenn Sie einen Administrator für genau einen virtuellen Administrationsserver zuweisen möchten, stellen Sie sicher, dass der Administrator keine Zugriffsrechte auf dem primären Administrationsserver hat.

Sie weisen einem virtuellen Administrationsserver einen Administrator zu, indem Sie dem Administrator die Zugriffsrechte auf den virtuellen Administrationsserver gewähren. Sie können die erforderlichen Zugriffsrechte auf eine der folgenden Arten erteilen:

- Die Zugriffsrechte des Administrators manuell konfigurieren

- Dem Administrator eine oder mehrere Benutzerrollen zuweisen

Um sich an der Kaspersky Security Center Web Console anzumelden, gibt ein Administrator eines virtuellen Administrationsservers den Namen, den Benutzernamen und das Passwort an. Kaspersky Security Center Web Console authentifiziert den Administrator und öffnet den virtuellen Administrationsserver, für den der Administrator die Zugriffsrechte besitzt. Der Administrator kann nicht zwischen Administrationsservern wechseln.

Erforderliche Vorrausetzungen

Stellen Sie vor dem Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der virtuelle Administrationsserver wurde erstellt.
- Auf dem primären Administrationsserver haben Sie für den Administrator, den Sie dem virtuellen Administrationsserver zuweisen möchten ein Konto erstellt.
- Sie besitzen die Berechtigung **Objekt-ACLs ändern** in dem Funktionsbereich **Allgemeine Funktionen → Benutzerberechtigungen**.

Manuelles Konfigurieren der Zugriffsrechte

So weisen Sie einem virtuellen Administrationsserver einen Administrator zu:

1. Gehen Sie im Hauptmenü zum erforderlichen virtuellen Administrationsserver:
   a. Klicken Sie rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol ( ).
   b. Wählen Sie den gewünschten Administrationsserver aus.
2. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.
   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
3. Klicken Sie auf der Registerkarte **Zugriffsrechte** auf die Schaltfläche **Hinzufügen**.
   Es öffnet sich eine zusammenfassende Liste der Benutzer des primären Administrationsservers und des aktuellen virtuellen Administrationsservers.
4. Wählen Sie aus der Benutzerliste das Konto des Administrators aus, das Sie dem virtuellen Administrationsserver zuweisen möchten, und klicken Sie anschließend auf die Schaltfläche **OK**.
   Die Anwendung fügt den ausgewählten Benutzer der Benutzerliste auf der Registerkarte **Zugriffsrechte** hinzu.
5. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Konto und klicken Sie auf die Schaltfläche **Zugriffsrechte**.
6. Konfigurieren Sie die Rechte, die der Administrator auf dem virtuellen Administrationsserver bekommen soll.
   Um sich erfolgreich anzumelden, muss der Administrator mindestens über die folgenden Berechtigungen verfügen:
   - Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen → Basisfunktionen**
   - Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen → Virtuelle Administrationsserver**

Die Anwendung speichert die geänderten Benutzerrechte im Administratorkonto.

Konfigurieren der Zugriffsrechte durch Zuweisen von Benutzerrollen

Alternativ können Sie einem Administrator des virtuellen Administrationsservers die Zugriffsrechte über Benutzerrollen zuweisen. Dies kann beispielsweise nützlich sein, wenn Sie mehrere Administratoren auf demselben virtuellen Administrationsserver zuweisen möchten. In diesem Fall können Sie den Konten der Administratoren die gleiche oder mehrere Benutzerrollen zuweisen, anstatt für mehrere Administratoren die gleichen Benutzerrechte zu konfigurieren.

So weisen Sie einem virtuellen Administrationsserver einen Administrator durch Zuweisung von Benutzerrollen zu:

1. Erstellen Sie eine neue Benutzerrolle auf dem primären Administrationsserver und legen Sie anschließend alle erforderlichen Zugriffsrechte fest, die ein Administrator auf dem virtuellen Administrationsserver bekommen soll. Sie können mehrere Rollen anlegen, wenn Sie beispielsweise den Zugriff auf verschiedene Funktionsbereiche trennen möchten.

2. Wechseln Sie im Hauptmenü zum erforderlichen virtuellen Administrationsserver:

   a. Klicken Sie rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol (▣).

   b. Wählen Sie den gewünschten Administrationsserver aus.

3. Weisen Sie die neue Rolle oder mehrere Rollen dem Administratorkonto zu.

   Die Anwendung weist dem Administratorkonto die neue Rolle zu.

Konfigurieren der Zugriffsrechte auf Objektebene

Neben der Zuweisung von Zugriffsrechten auf Ebene von Funktionsbereichen können Sie auch den Zugriff auf bestimmte Objekte konfigurieren, die sich auf dem virtuellen Administrationsserver befinden, beispielsweise einer bestimmten Administrationsgruppe oder Aufgabe. Wechseln Sie dazu auf den virtuellen Administrationsserver und konfigurieren Sie anschließend die Zugriffsrechte in den Eigenschaften des Objekts.

Administrationsserver für Client-Geräte wechseln

Mit der Aufgabe *Administrationsserver wechseln* wechseln können Sie den Administrationsserver, der die Client-Geräte verwaltet, durch einen anderen Administrationsserver ersetzen. Nach Abschluss der Aufgabe werden die Client-Geräte unter die Verwaltung des Administrationsservers gestellt, denn Sie angegeben haben.

Sie können die Aufgabe *Administrationsserver wechseln* nicht für Client-Geräte verwenden, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind. Für solche Geräte müssen Sie entweder den Administrationsagenten neu konfigurieren oder den Administrationsagenten neu installieren und das Verbindungs-Gateway angeben.

So ändern Sie einen Administrationsserver, der die Client-Geräte verwaltet:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.

3. Geben Sie im Schritt **Einstellungen der neue Aufgabe** des Assistenten die folgenden Einstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Programm** die Option **Kaspersky Security Center** aus.

   b. Wählen Sie im Feld **Aufgabentyp** die Option **Administrationsserver wechseln** aus.

   c. Geben Sie im Feld **Aufgabenname** den Namen für die Aufgabe an, die Sie erstellen.

   Der Aufgabenname darf höchstens 100 Zeichen lang sein und darf keine Sonderzeichen ("*<>?\:|) enthalten.

   d. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

     Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

4. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** des Assistenten eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

5. Bestätigen Sie in diesem Schritt des Assistenten, dass Sie den Bedingungen für das Wechseln des Administrationsservers für Client-Geräte zustimmen.

6. Wählen Sie in diesem Schritt des Assistenten den Administrationsserver aus, den Sie für die Verwaltung der ausgewählten Geräte verwenden möchten:

   - **Zu einem anderen primären Administrationsserver wechseln**

     Um Client-Geräte auf einen anderen primären Administrationsserver zu verschieben, geben Sie die folgenden Verbindungseinstellungen für den Administrationsserver an:

     1. Geben Sie im Feld **Adresse des Administrationsservers** die Adresse des neuen primären Administrationsservers an.

     2. Geben Sie im Feld **Port** die Portnummer für die Verbindung zum Administrationsserver an.

        Standardmäßig wird die Portnummer 14000 verwendet.

     3. Geben Sie im Feld **SSL-Port** die Nummer des SSL-Ports auf dem primären Administrationsserver an

        Standardmäßig wird die Portnummer 13000 verwendet.

     4. Aktivieren Sie bei Bedarf die Option **Proxyserver verwenden**.

        Wenn diese Option deaktiviert ist, wird die direkte Verbindung genutzt, um das Gerät mit dem Administrationsserver zu verbinden.

        Wenn diese Option aktiviert ist, geben Sie die Parameter des Proxyservers an:

        - **Proxyserver-Adresse**

        - **Proxyserver-Port**

        Falls Ihr Proxyserver eine Authentifizierung erfordert, geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldeinformationen des Kontos ein, unter dem die Verbindung mit dem Proxyserver hergestellt wird. Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

     5. Laden Sie bei Bedarf ein neues Zertifikat für den Administrationsserver hoch.

   - **Auf diesem primären Server zu einem anderen virtuellen Server wechseln**

     Wählen Sie diese Option aus, um die Client-Geräte zu einem virtuellen Administrationsserver auf dem aktuellen primären Administrationsserver verschieben. Wählen Sie dazu in der Dropdown-Liste **Name des virtuellen Administrationsservers** den gewünschten virtuellen Administrationsserver aus.

7. Geben Sie im Schritt **Benutzerkonto für die Ausführung der Aufgabe auswählen** des Assistenten die Kontoeinstellungen an:

   - **Standardbenutzerkonto**

     Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

     Diese Variante ist standardmäßig ausgewählt.

- **Benutzerkonto festlegen**

  Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

  - **Benutzerkonto**

    Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

  - **Kennwort**

    Kennwort des Benutzerkontos, unter dem die Aufgabe ausgeführt wird.

8. Wenn Sie die standardmäßigen Aufgabeneinstellungen ändern möchten, aktivieren Sie auf in dem Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**.

   Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

10. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

11. Wenn Sie die standardmäßigen Aufgabeneinstellungen ändern möchten, geben Sie im Fenster mit den Aufgabeneigenschaften die allgemeinen Aufgabeneinstellungen entsprechend Ihren Bedürfnissen an.

12. Klicken Sie auf die Schaltfläche **Speichern**.

    Die Aufgabe wird erstellt und konfiguriert.

13. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe werden die Client-Geräte, für welche die Aufgabe erstellt wurde, auf den Administrationsserver umgestellt, der in den Einstellungen der Aufgabe angegeben wurde.

Einen virtuellen Administrationsserver löschen

Wenn Sie einen virtuellen Administrationsserver löschen, werden auch alle Objekte gelöscht, die auf dem virtuellen Administrationsserver erstellt wurden, inklusive Richtlinien und Aufgaben. Die verwalteten Geräte aus den Administrationsgruppen, die von dem virtuellen Administrationsserver verwaltet wurden, werden von den Administrationsgruppen entfernt. Um die Geräte erneut in die Verwaltung durch Kaspersky Security Center aufzunehmen, müssen Sie eine Netzwerkabfrage durchführen und die gefundenen Geräte von der Gruppe "Nicht zugeordnete Geräte" in die Administrationsgruppe verschieben.

So löschen Sie einen virtuellen Administrationsserver:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol () neben dem Namen des Administrationsservers.

2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.

3. Wählen Sie den virtuellen Administrationsserver aus, den Sie löschen möchten.

4. Klicken Sie in der Menüleiste auf **Löschen**.

Der virtuelle Administrationsserver wurde gelöscht.

Aktivieren des Benutzerkonten-Schutzes vor unbefugten Änderungen

Sie können eine zusätzliche Option aktivieren, um ein Benutzerkonto vor unbefugten Änderungen zu schützen. Wenn diese Option aktiviert ist, muss sich der Benutzer mit Änderungsrechten autorisieren, um die Benutzerkonto-Einstellungen zu ändern.

Um den Benutzerkonten-Schutz vor unbefugten Änderungen zu aktivieren oder zu deaktivieren:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer**.

2. Klicken Sie auf den Namen des internen Benutzerkontos, für das Sie den Benutzerkonten-Schutz vor nicht autorisierten Änderungen anpassen möchten.

3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.

4. Wählen Sie auf der Registerkarte **Schutz des Benutzerkontos** die Option **Authentifizierung verlangen, um die Berechtigung zum Ändern von Benutzerkonten zu überprüfen**, wenn Sie jedes Mal Anmeldedaten anfordern möchten, sobald Benutzerkonto-Einstellungen geändert oder bearbeitet werden. Wählen Sie andernfalls die Option **Benutzern das Ändern des Kontos ohne zusätzliche Authentifizierung erlauben**.

5. Klicken Sie auf **Speichern**.

Der Schutz vor unbefugten Änderungen für ein Benutzerkonto ist aktiviert.

Backup-Kopie der Daten des Administrationsservers anlegen und wiederherstellen

Ein Daten-Backup ermöglicht es Ihnen, den Administrationsserver ohne Datenverlust von einem Gerät auf ein anderes zu übertragen. Mittels eines Backups können Sie Daten wiederherstellen, wenn Sie die Administrationsserver-Datenbank auf ein anderes Gerät verschieben oder auf eine aktuellere Version von Kaspersky Security Center aktualisieren. Darüber hinaus erlaubt die Verwendung eines Daten-Backups das Verschieben der Daten des Administrationsservers von Kaspersky Security Center Windows unter die Verwaltung von Kaspersky Security Center Linux (ein Verschieben der Daten von Kaspersky Security Center Linux zu Kaspersky Security Center Windows wird nicht unterstützt).

Die installierten Verwaltungs-Plug-ins werden nicht mittels Backup gesichert. Nachdem Sie die Daten des Administrationsservers aus einer Sicherungskopie wiederhergestellt haben, müssen Sie Plug-ins für die verwalteten Anwendungen herunterladen und neu installieren.

Bevor Sie ein Backup des Administrationsservers erstellen, prüfen Sie, ob ein virtueller Administrationsserver zur Administrationsgruppe hinzugefügt wurde. Sollte ein virtueller Administrationsserver hinzugefügt worden sein, stellen Sie vor dem Backup sicher, dass dem virtuellen Administrationsserver ein Administrator zugewiesen ist. Nach dem Backup können Sie für den virtuellen Administrationsserver keine Administratorrechte mehr vergeben. Beachten Sie, dass im Sie im Falle des Verlusts der Anmeldeinformationen des Administrators nicht mehr in der Lage sind, dem virtuellen Administrationsserver einen neuen Administrator zuzuweisen.

Um einen Failover-Cluster für Kaspersky Security Center zu sichern oder wiederherzustellen, müssen Sie den gesamten Cluster zu Wartungszwecken anhalten und ihn nach Abschluss der Sicherung oder Wiederherstellung neu starten.

Sie können eine Backup-Kopie der Daten des Administrationsservers auf eine der folgenden Weisen erstellen:

- Eine Aufgabe zum Anlegen eines Daten-Backups über die Verwaltungskonsole erstellen und starten.
- Das Tool klbackup auf einem Gerät mit dem installierten Administrationsserver starten. Dieses Tool gehört zum Lieferumfang von Kaspersky Security Center. Es befindet sich nach der Installation des Administrationsservers im Stammverzeichnis des Zielordners, der bei der Installation angegeben wurde.

In der Backup-Kopie der Daten des Administrationsservers werden folgende Daten gespeichert:

- Administrationsserver-Datenbank (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse).
- Konfigurationsdaten über die Struktur der Administrationsgruppen und Client-Geräte.
- Speicherort der Programmpakete für die Remote-Installation.
- Zertifikat des Administrationsservers.

- Inhalt des Ordners *Updates*.

  Der Ordnerpfad lautet standardmäßig C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Die Wiederherstellung von Daten des Administrationsservers ist nur mithilfe des Hilfsprogramms klbackup möglich. Sie müssen die Wiederherstellung auf einer funktionierenden Instanz des Administrationsservers durchführen, die gerade installiert wurde und die gleiche Version (oder höher) besitzt, für welche die Sicherung erstellt wurde.

Aufgabe zum Anlegen eines Backups

Die Aufgabe zum Anlegen eines Backups gehört zu den Aufgaben des Administrationsservers und wird vom Schnellstartassistenten erstellt. Wenn die vom Schnellstartassistenten erstellte Aufgabe zum Anlegen eines Backups gelöscht wurde, können Sie diese manuell erstellen.

Um eine Aufgabe zum Anlegen eines Backups des Administrationsservers zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Fenster **Einstellungen der neue Aufgabe** des Assistenten den Aufgabentyp **Backup der Daten des Administrationsservers anlegen** aus.
4. Folgen Sie den weiteren Schritten des Assistenten.

Die Aufgabe **Backup der Daten des Administrationsservers anlegen** kann nur einmal angelegt werden. Wenn die Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers für den Administrationsserver bereits erstellt wurde, wird sie im Fenster für die Auswahl des Aufgabentyps des Assistenten für das Erstellen einer Aufgabe zum Anlegen eines Backups nicht angezeigt.

So konfigurieren Sie die Aufgabe zum Anlegen eines Backups der Daten des Administrationsservers:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben** und wählen Sie anschließend die Aufgabe **Backup der Daten des Administrationsservers anlegen** aus.
2. Klicken Sie auf die Aufgabe **Backup der Daten des Administrationsservers anlegen**

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
3. Passen Sie bei Bedarf die allgemeinen Aufgabeneinstellungen gemäß Ihren Anforderungen an.
4. Geben Sie im Abschnitt **Programmeinstellungen** den Pfad des Ordners für die Backup-Kopien der Daten des Administrationsservers, das Kennwort für den Schutz des Backups und die Anzahl der Backup-Kopien (bei Bedarf) an.
5. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Die Aufgabe *Backup der Daten des Administrationsservers anlegen* ist konfiguriert.

Administrationsserver auf anderes Gerät übertragen

Wenn Sie den Administrationsserver auf einem neuen Gerät verwenden müssen, können Sie ihn auf eine der folgenden Arten verschieben:

- Verschieben Sie den Administrationsserver und den Datenbankserver auf ein neues Gerät (der Datenbankserver kann auf dem neuen Gerät zusammen mit dem Administrationsserver oder auf einem anderen Gerät installiert werden).
- Belassen Sie den Datenbankserver auf dem bisherigen Gerät und verschieben Sie nur den Administrationsserver auf ein neues Gerät.

So verschieben Sie Administrationsserver und den Datenbankserver auf ein neues Gerät:

1. Erstellen Sie auf dem bisherigen Gerät ein Backup der Daten des Administrationsservers.

   Dazu können Sie entweder die Datensicherungsaufgabe über Kaspersky Security Center Web Console ausführen oder das Dienstprogramm klbackup ausführen.

   > Wenn Sie derzeit SQL Server als DBMS für den Administrationsserver verwenden, können Sie die Daten von SQL Server zu MySQL oder MariaDB DBMS migrieren. Führen Sie dazu das Tool "klbackup" im interaktiven Modus aus, um ein Daten-Backup zu erstellen. Aktivieren Sie die Option **Auf MySQL/MariaDB-Format migrieren** im Fenster **Einstellungen für Backups** des Backup- und Wiederherstellungsassistenten. Kaspersky Security Center erstellt ein mit MySQL und MariaDB kompatibles Backup. Danach können Sie die Daten aus dem Backup in MySQL oder MariaDB wiederherstellen.

   > Sie können auch die Option **Auf Azure-Format migrieren** aktivieren, wenn Sie die Daten von SQL Server zu Azure SQL DBMS migrieren wollen.

2. Trennen Sie den Administrationsserver auf dem vorherigen Gerät vom Netzwerk.

3. Wählen Sie ein neues Gerät aus, auf dem der Administrationsserver installiert werden soll. Stellen Sie sicher, dass die Hardware und Software des ausgewählten Gerätes den Anforderungen für den Administrationsserver, für Kaspersky Security Center Web Console und für den Administrationsagenten entsprechen. Überprüfen Sie außerdem, ob die auf dem Administrationsserver verwendeten Ports verfügbar sind.

4. Weisen Sie dem neuen Gerät dieselbe Adresse zu.

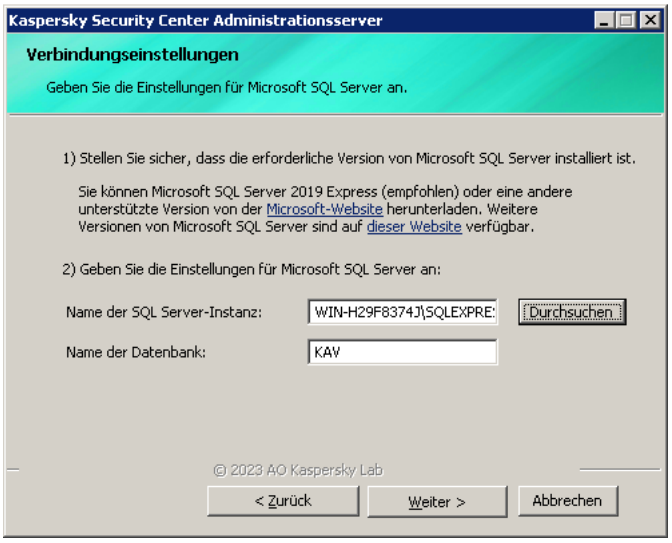
   Dem neuen Administrationsserver können der NetBIOS-Name, der FQDN und die statische IP-Adresse zugewiesen werden. Dies hängt davon ab, welche Adresse für den Administrationsagenten im Installationspaket des Administrationsagenten angegeben wurde, als die Administrationsagenten verteilt wurden. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools klnagchk ermittelt werden).

5. Installieren Sie das Datenbankverwaltungssystem (DBMS) bei Bedarf auf einem anderen Gerät, das vom Administrationsserver verwenden wird.

   Die Datenbank kann entweder zusammen mit dem Administrationsserver auf dem neuen Gerät oder auf einem anderen Gerät installiert werden. Stellen Sie sicher, dass dieses Gerät die Hard- und Softwarevoraussetzungen erfüllt. Berücksichtigen Sie bei der Auswahl eines DBMS die Anzahl der Geräte, die vom Administrationsserver verwaltetet werden.

6. Führen Sie auf dem neuen Gerät die Installation des Administrationsservers aus.

7. Konfigurieren Sie die Verbindungseinstellungen des Datenbankservers während der Installation des Administrationsservers.



Beispiel für das Fenster mit den Verbindungseinstellungen für Microsoft SQL Server

Führen Sie je nachdem, wo Sie den Datenbankserver platzieren müssen, einen der folgenden Schritte aus:

- **Belassen Sie den Datenbankserver auf dem vorherigen Gerät**

  1. Klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Name der SQL Server-Instanz** und wählen Sie in der angezeigten Liste den vorherigen Gerätenamen.

     Beachten Sie, dass das vorherige Gerät für die Verbindung mit dem neuen Administrationsserver verfügbar sein muss.

  2. Geben Sie den vorherigen Datenbanknamen im Feld **Name der Datenbank** ein.

- **Verschieben Sie den Datenbankserver auf das andere Gerät**

  1. Klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Name der SQL Server-Instanz** und wählen Sie anschließend den Gerätenamen, der in der Liste angezeigt wird.

  2. Geben Sie denen neuen Datenbankname im Feld **Name der Datenbank** ein.

     Beachten Sie, dass der neue Datenbankname mit dem Namen der Datenbank des vorherigen Geräts übereinstimmen muss. Die Namen der Datenbanken müssen identisch sein, damit Sie die Sicherung des Administrationsservers verwenden können. Der Standarddatenbankname ist *KAV*.

8. Stellen Sie nach Abschluss der Installation die Administrationsserver-Daten auf dem neuen Gerät mithilfe des Dienstprogramms klbackup wieder her.

   Wenn Sie als DBMS auf dem vorherigen und neuen Gerät SQL Server verwenden, beachten Sie, dass die auf dem neuen Gerät installierte Version von SQL Server mit der auf dem vorherigen Gerät installierten Version von SQL Server identisch oder höher sein muss. Andernfalls können Sie die Daten des Administrationsservers auf dem neuen Gerät nicht wiederherstellen.

9. Öffnen Sie die Kaspersky Security Center Web Console und stellen Sie eine Verbindung zum Administrationsserver her.

10. Überprüfen Sie, ob alle verwalteten Geräte mit dem Administrationsserver verbunden sind.

11. Deinstallieren Sie den Administrationsserver und den Datenbankserver vom bisherigen Gerät.

Sie können außerdem die Verwaltungskonsole verwenden, um den Administrationsserver und einen Datenbankserver auf ein anderes Gerät zu verschieben.

Integrität der Module anhand der Tools klscmodchk und integrity_checker prüfen

Kaspersky Security Center enthält mehrere Binärmodule in Form von dynamisch verlinkten Bibliotheken, ausführbaren Dateien, Konfigurationsdateien und Schnittstellendateien. Eindringlinge können eine oder mehrere ausführbare Dateien oder Anwendungsdateien durch Dateien mit schädlichem Code ersetzen. Um das Ersetzen von Modulen oder Dateien zu verhindern, bietet Kaspersky Security Center mit den Tools "klscmodchk" und "integrity_checker" eine Integritätsprüfung für Komponenten. Diese Tools prüfen Module und Dateien auf unbefugte Änderungen oder Beschädigungen. Wenn die Prüfsumme eines Moduls oder einer Anwendung nicht korrekt ist, gilt das Modul oder die Anwendung als beschädigt.

Das Tool "klscmodchk" führt die Integritätsprüfungen für die folgenden Komponenten von Kaspersky Security Center durch:

- Administrationsserver
- Administrationsagent
- Verwaltungs-Plug-ins für die Verwaltungskonsole mit Manifest-Dateien

Das Tool "integrity_checker" führt die Integritätsprüfungen für die folgenden Komponenten von Kaspersky Security Center durch:

- Administrationsserver
- Administrationsagent
- Kaspersky Security Center Web Console

Beide Tools prüfen die Integrität auf Grundlage der Manifest-Datei "kl_file_integrity_manifest.xml", die ein Teil der Build-Version von Kaspersky Security Center ist und sich im Installationsordner befindet. Die Komponenten-Manifest-Datei enthält Dateien, deren Integrität für den ordnungsgemäßen Betrieb von Kaspersky Security Center wichtig ist. Die Integrität der Manifest-Dateien wird ebenfalls geprüft.

Es wird dringend empfohlen, die Manifest-Datei "kl_file_integrity_manifest.xml" nicht zu verändern, da dies die digitalen Signaturen ungültig macht und die Integritätsprüfung fehlschlagen lässt.

Um die Integrität von Kaspersky Security Center zu prüfen, führen Sie einen der folgenden Befehle aus:

- `$ klscmodchk [ Parameter ]`

  Das Tool "klscmodchk" startet das Tool "integrity_checker" mit dem Parameter `--verbose` und prüft die Integrität der Module.

Parameter des Tools "klscmodchk":

- `-logfile <log_file_path>` – Geben Sie zum Loggen den Pfad einer Datei auf der Festplatte an. Standardmäßig erfolgt die Ausgabe über die Konsole.
- `-chkplugins` – Überprüft die Integrität von installierten Verwaltungs-Plug-ins für eine Verwaltungskonsole, die Manifestdateien enthält. Standardmäßig werden die Verwaltungs-Plug-ins nicht überprüft.
- `-verbose` – Ausgeben von erweiterten Informationen während der Integritätsprüfung.

- `$ integrity_checker [ Parameter ] <Pfad zur Manifest-Datei>`

  Parameter des Tools "integrity_checker":

  - `--help` – Anzeigen der Hilfe des Tools "integrity_checker".
  - `--version` – Anzeigen der Versionsnummer des Tools "integrity_checker".
  - `--verbose` – Anzeigen von Informationen zur Ausführung des Tools. Bei der Durchführung einer Integritätsprüfung ist es ausreichend, diesen Parameter im Befehl zu verwenden.

Das Ergebnis der Prüfung wird für jede Manifest-Datei neben ihrem Namen im folgenden Format angezeigt:

- SUCCEEDED – Die Integrität der Datei wurde bestätigt (Rückgabe-Code 0).
- FAILED – Die Integrität der Datei wurde nicht bestätigt (Rückgabe-Code von null abweichend).

Sie können Integritätsprüfungen auch so konfigurieren, dass sie automatisch gestartet werden, wenn Sie die Anwendung starten. Standardmäßig ist die automatische Integritätsprüfung deaktiviert.

So aktivieren Sie die automatische Integritätsprüfung:

1. Geben Sie auf dem Gerät mit dem installierten Administrationsserver in der Windows-Befehlszeile den folgenden Befehl ein:

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Starten Sie das Gerät neu.

Die automatische Integritätsprüfung ist aktiviert.

Beim nächsten Start von Kaspersky Security Center wird das Tool "klscmodchk" zusammen mit dem Administrationsserver ausgeführt und startet die Integritätsprüfung der Module. Die Ergebnisse der Integritätsprüfungen werden in das Kaspersky-Ereignisprotokoll geschrieben.

Erstkonfiguration von Kaspersky Security Center Web Console

In diesem Abschnitt werden die Schritte beschrieben, die Sie nach der Installation von Kaspersky Security Center Web Console zur Ersteinrichtung des Programms ausführen müssen.

Schnellstartassistent (Kaspersky Security Center Web Console)

Dieser Abschnitt enthält Informationen zum Schnellstartassistenten für den Administrationsserver.

Der Assistent benötigt einen Internetzugang. Wenn Ihr Administrationsserver keinen Internetzugang besitzt, empfehlen wir Ihnen, alle Schritte des Assistenten manuell über die Benutzeroberfläche der Kaspersky Security Center Web Console auszuführen.

Mit Kaspersky Security Center können Sie eine minimale Auswahl von Einstellungen anpassen, die für den Aufbau eines zentralisierten Verwaltungssystems für den Schutz Ihres Netzwerks vor Bedrohungen erforderlich sind. Diese Konfiguration wird mithilfe des Schnellstartassistenten für das Programm durchgeführt. Während der Ausführung des Assistenten können Sie die folgenden Änderungen an der Anwendung vornehmen:

- Schlüsseldateien hinzufügen oder Aktivierungscodes eingeben, die automatisch auf die Geräte der Administrationsgruppen verteilt werden können.
- Interaktion mit Kaspersky Security Network (KSN) konfigurieren. Bei erlaubter Verwendung von KSN aktiviert der Assistent den Dienst des KSN-Proxyservers, mit dem die Interaktion zwischen KSN und den Geräten gewährleistet wird.
- E-Mail-Versand von Benachrichtigungen über Ereignisse konfigurieren, die vom Administrationsserver und den verwalteten Programmen registriert werden. (Damit Benachrichtigungen erfolgreich zugestellt werden, muss auf dem Administrationsserver und auf allen Geräten der Windows Messenger Dienst gestartet werden.)
- Schutzrichtlinien für Arbeitsstationen und Server sowie Aufgaben zur Schadsoftware-Untersuchung, Update-Download und Verschieben ins Backup für die oberste Hierarchieebene der verwalteten Geräte erstellen.

  Der Schnellstartassistent erstellt Richtlinien nur für die Anwendungen, deren Ordner **Verwaltete Geräte** noch keine Richtlinien enthält. Der Schnellstartassistent erstellt keine Aufgaben, deren Namen mit den Aufgabennamen übereinstimmen, die für die obere Hierarchieebene der verwalteten Geräte bereits erstellt wurden.

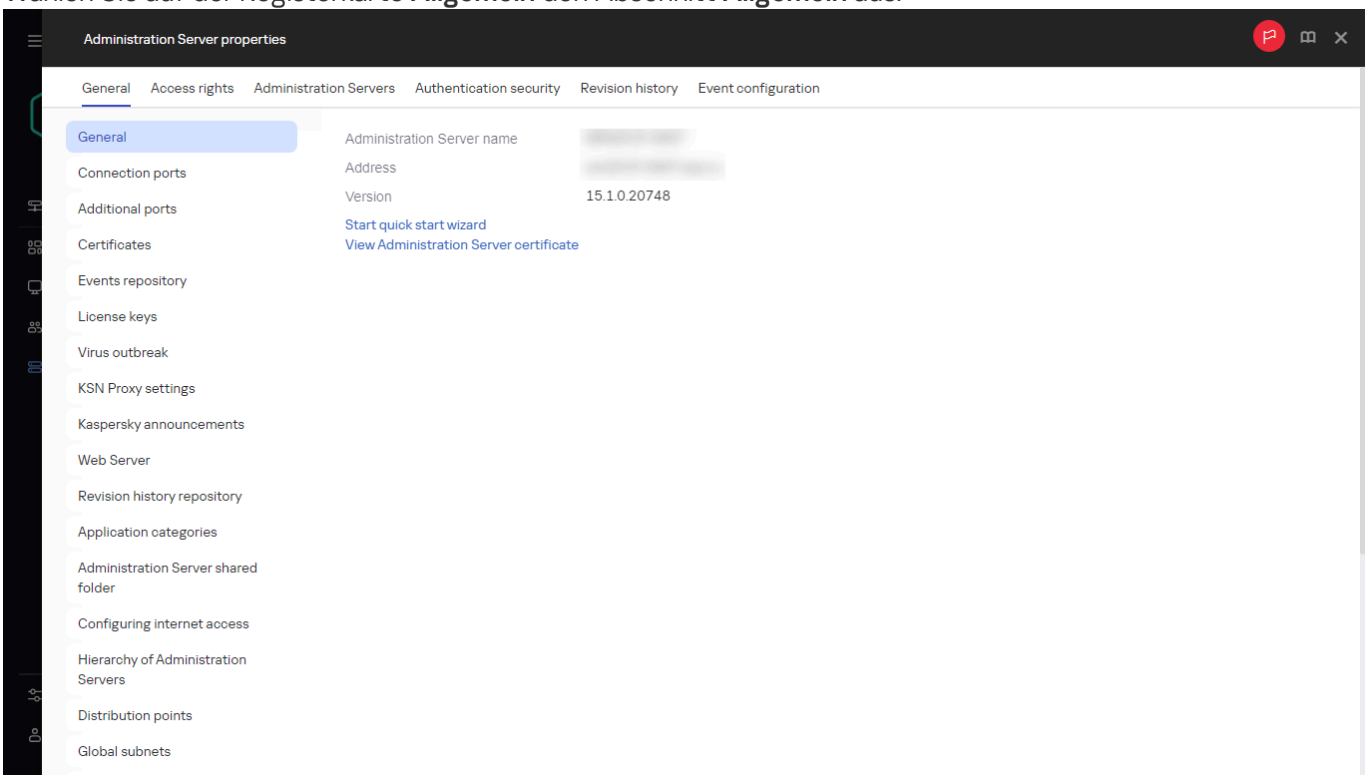
Die Anwendung schlägt automatisch vor, beim ersten Verbindungsaufbau zum Server nach der Installation des Administrationsservers den Schnellstartassistenten zu starten. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

So starten Sie den Schnellstartassistenten manuell:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Allgemein** aus.



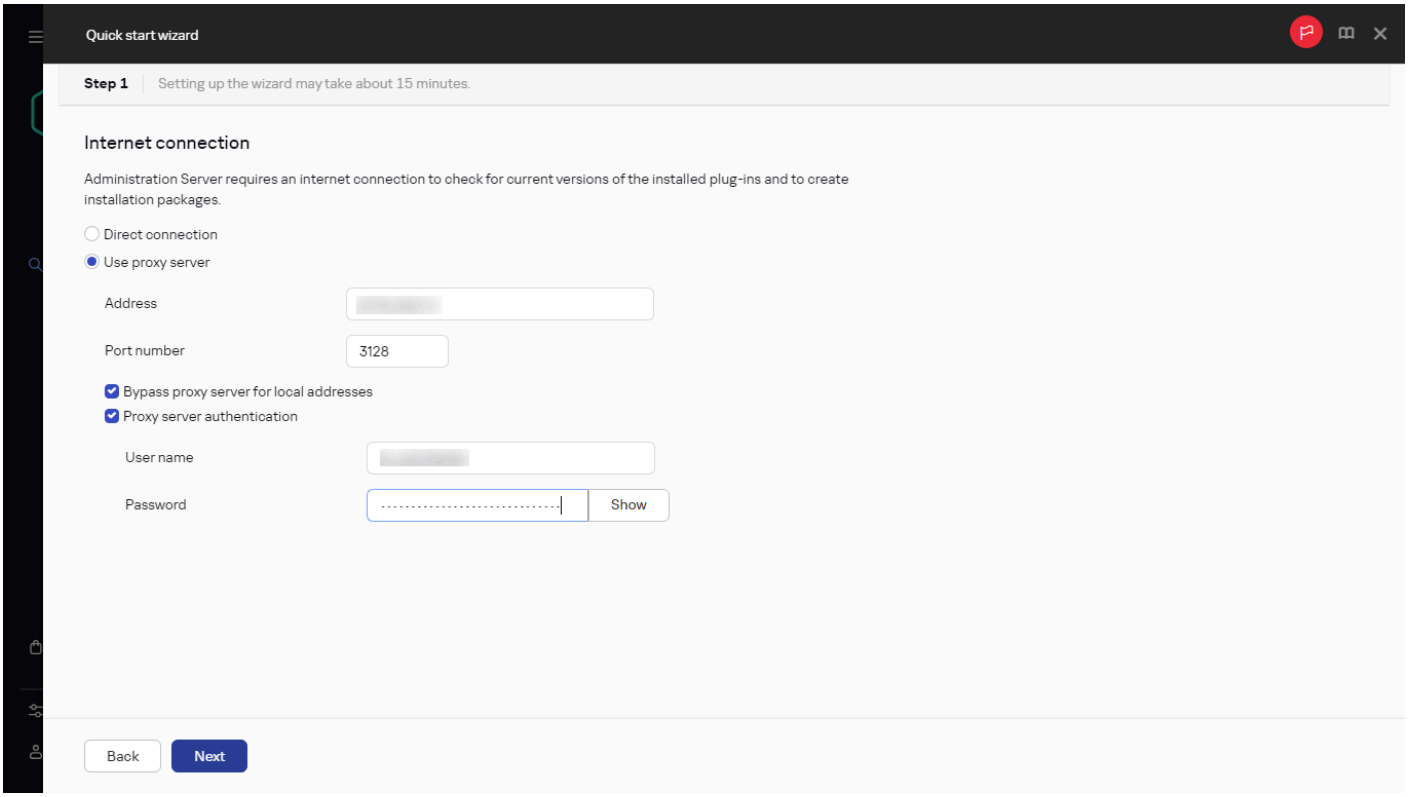
Eigenschaftenfenster des Administrationsservers

3. Klicken Sie auf die Schaltfläche **Schnellstartassistent starten**.

Der Assistent schlägt vor, die ursprünglichen Einstellungen des Administrationsservers zu generieren. Folgen Sie den Anweisungen des Assistenten. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

Schritt 1. Einstellungen für die Internetverbindung festlegen

Geben Sie die Internetzugriffseinstellungen für den Administrationsserver an. Sie müssen den Internetzugang anpassen, um Kaspersky Security Network zu verwenden und um Updates für die Antiviren-Datenbanken von Kaspersky Security Center und die verwalteten Kaspersky-Anwendungen herunterzuladen.



Einstellungen der Internetverbindung

Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

- **Adresse**

  Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center mit dem Internet.

- **Port**

  Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center hergestellt wird.

- **Proxyserver für lokale Adressen umgehen**

  Bei der Verbindung mit den Geräten im lokalen Netzwerk wird kein Proxyserver verwendet.

- **Authentifizierung am Proxyserver**

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver verwenden** aktiviert ist.

- **Benutzername**

  Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

- **Kennwort**

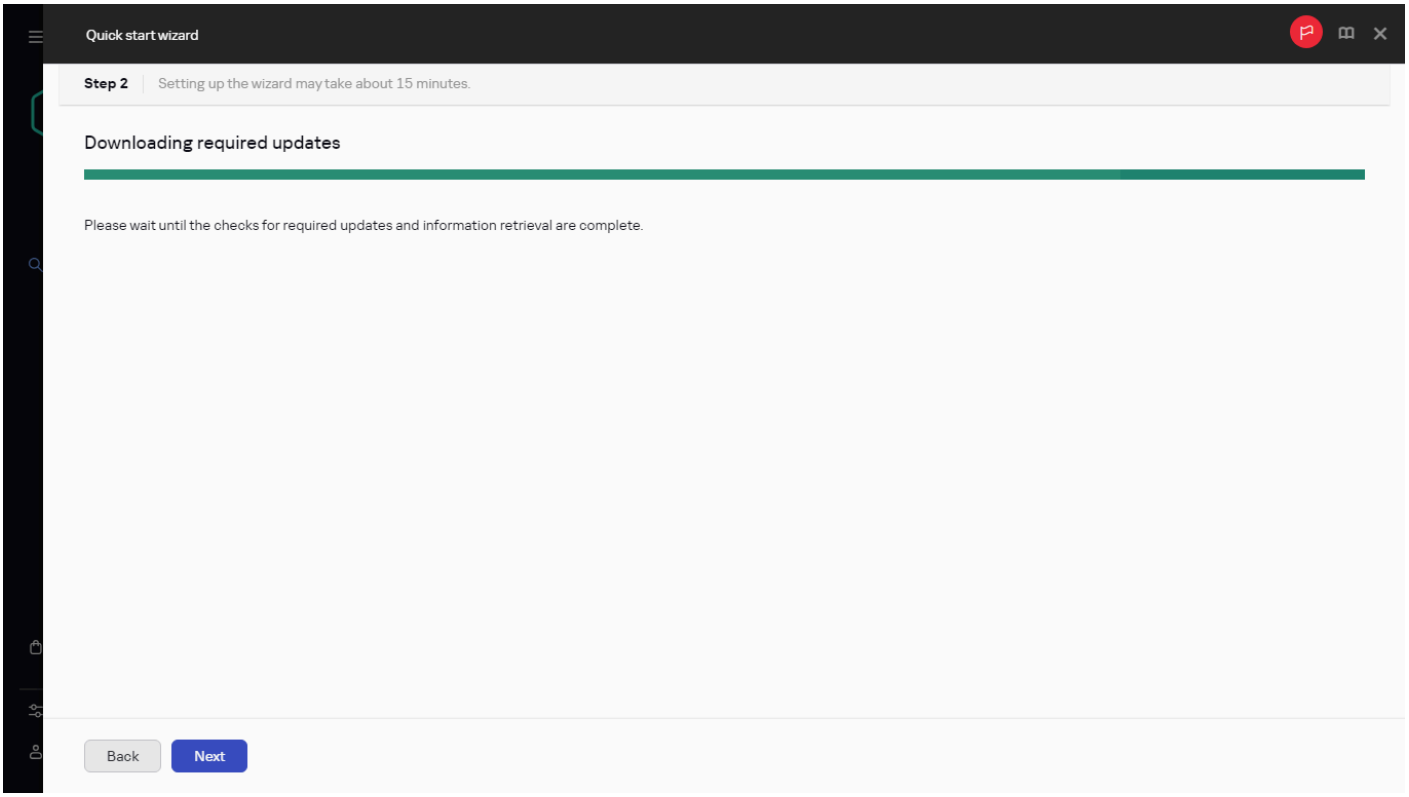
  Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

  Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

Das Konfigurieren des Internetzugriffs ist auch später, unabhängig vom Schnellstartassistenten, möglich.

Schritt 2. Erforderliche Updates herunterladen

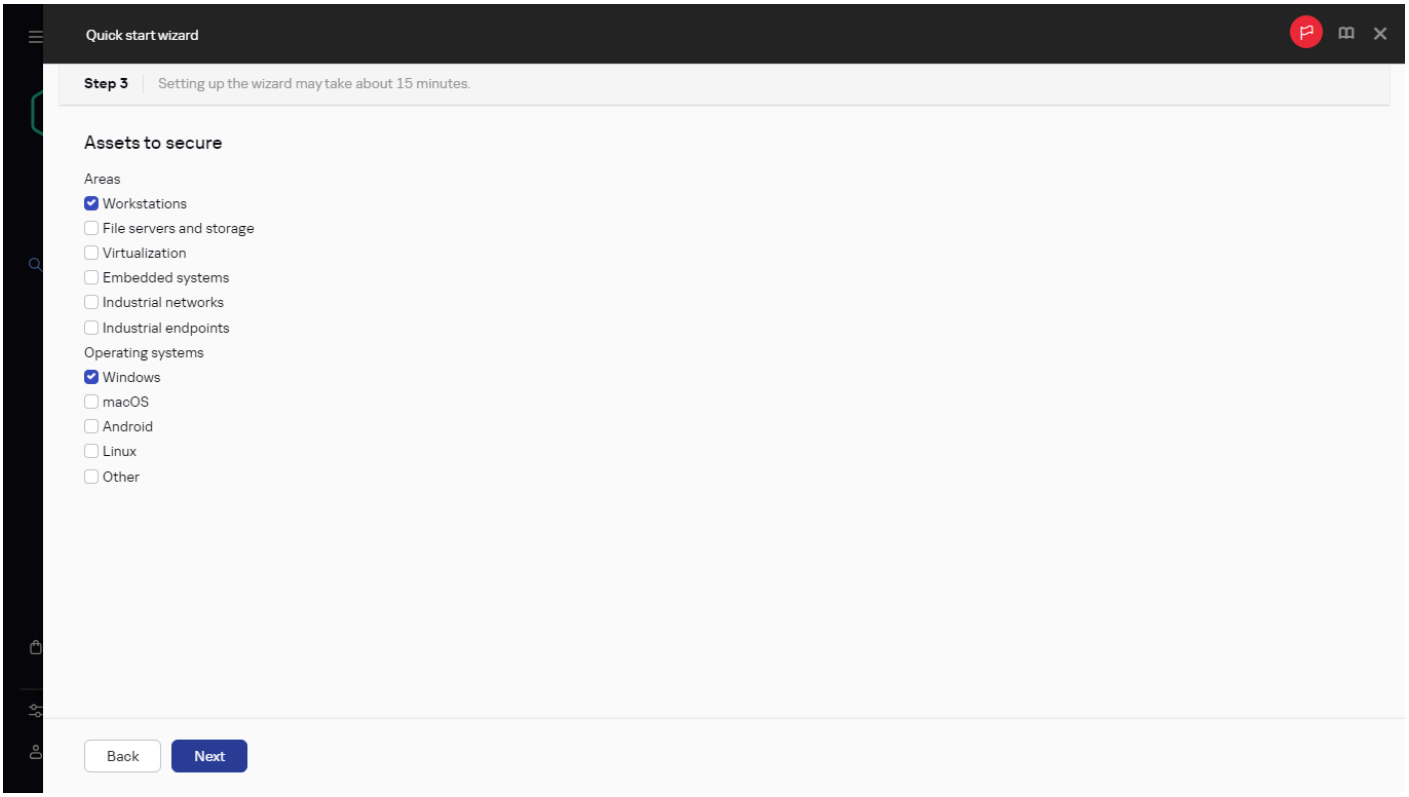
Die erforderlichen Updates werden automatisch von den Kaspersky-Servern heruntergeladen.



Erforderliche Updates herunterladen

Schritt 3. Zu sichernde Assets auswählen

Wählen Sie die Schutzbereiche und Betriebssysteme aus, die Sie in Ihrem Netzwerk verwenden. Geben Sie bei der Auswahl die Filter für die Plug-ins zur Anwendungsverwaltung und für die Programmpakete auf den Kaspersky-Servern an, die Sie herunterladen und auf Client-Geräten in Ihrem Netzwerk installieren können.



Zu sichernde Assets auswählen

Wählen Sie die Optionen aus:

- **Bereiche**

  Sie können die folgenden Schutzbereiche auswählen:

  - **Workstations**. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk Workstations schützen möchten. Standardmäßig ist die Variante "Workstations" ausgewählt.

  - **Dateiserver und Datenspeicherungssysteme**. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk Dateiserver schützen möchten.

  - **Mobile Geräte**. Wählen Sie diese Option aus, wenn Sie mobile Geräte schützen möchten, die dem Unternehmen oder den Unternehmensmitarbeitern gehören. Wenn Sie diese Option auswählen, aber keine Lizenz für die Funktion "Verwaltung mobiler Geräte" bereitgestellt haben, wird gemeldet, dass eine Lizenz mit der Funktion "Verwaltung mobiler Geräte" bereitgestellt werden muss. Wenn Sie keine Lizenz bereitstellen, können Sie die Funktion "Verwaltung mobiler Geräte" nicht verwenden.

  - **Virtualisierungen**. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk virtuelle Maschinen schützen möchten.

  - **Kaspersky Anti-Spam**. Wählen Sie diese Option aus, wenn Sie die Mail-Server Ihres Unternehmens vor Spam, Betrug und Schadsoftware schützen möchten.

- **Embedded Systeme**. Wählen Sie diese Option aus, wenn Sie Windows-basierte Embedded-Systeme wie Geldautomaten (ATMs) schützen möchten.
- **Industrielle Netzwerke**. Wählen Sie diese Option, wenn Sie Sicherheitsdaten in Ihrem industriellen Netzwerk und von Netzwerkendpunkten überwachen möchten, die durch Kaspersky-Anwendungen geschützt sind.
- **Industrielle Endpoints**. Wählen Sie diese Option, wenn Sie individuelle Knoten innerhalb eines industriellen Netzwerks schützen möchten.

- **Betriebssysteme**

  Sie können die folgende Plattformen auswählen:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Sonstige

  Informationen zu den unterstützten Betriebssystemen finden Sie im Abschnitt "Hardware- und Softwarevoraussetzungen für die Kaspersky Security Center Web Console".

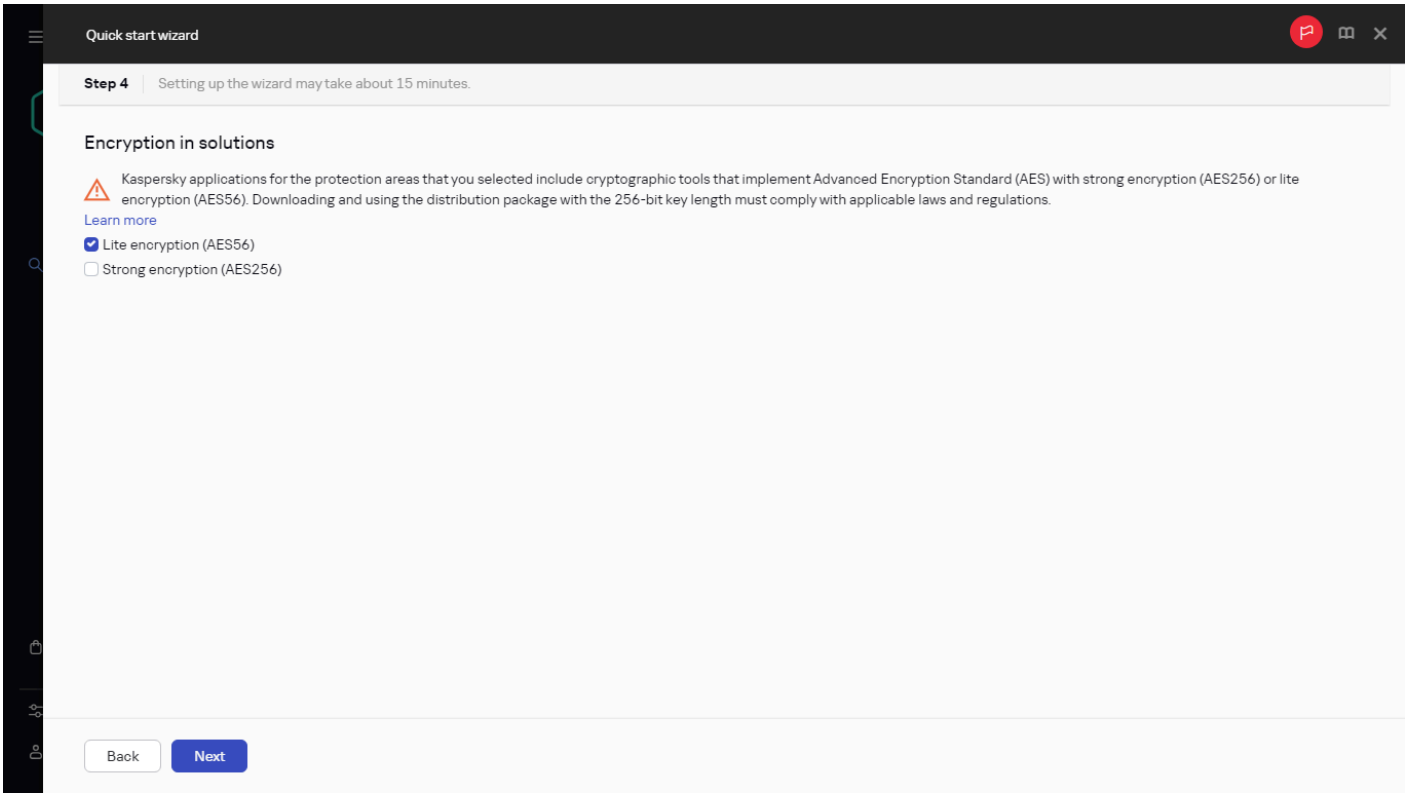
Das Auswählen der Pakete der Kaspersky-Anwendungen aus der Liste der verfügbaren Pakete kann später unabhängig vom Schnellstartassistenten durchgeführt werden. Um die Suche nach den benötigten Paketen zu vereinfachen, können Sie die Liste der verfügbaren Pakete nach verschiedenen Kriterien filtern.

Schritt 4. Verwendete Verschlüsselung für die Lösungen auswählen

Das Fenster **Angebotene Verschlüsselungen** wird nur angezeigt, wenn Sie **Workstations** als einen Schutzbereich ausgewählt haben.

Kaspersky Endpoint Security für Windows enthält Verschlüsselungs-Tools für die Informationen, die auf Windows-basierten Client-Geräten gespeichert werden. Diese Tools Verschlüsselungswerkzeuge, die den Advanced Encryption Standard (AES) mit einer 256-Bit oder 56-Bit Schlüssellänge implementiert haben.

Das Herunterladen und die Verwendung des Programmpakets mit einer 256-Bit-Schlüssellänge muss in Übereinstimmung mit den geltenden Gesetzen und Vorschriften erfolgen. Um ein Programmpaket von Kaspersky Endpoint Security für Windows herunterzuladen, dass den Bedürfnissen Ihrer Organisation entspricht, konsultieren Sie die Gesetzgebung in dem Land, in dem sich die Client-Geräte Ihrer Organisation befinden.



Verwendete Verschlüsselung für die Lösungen auswählen

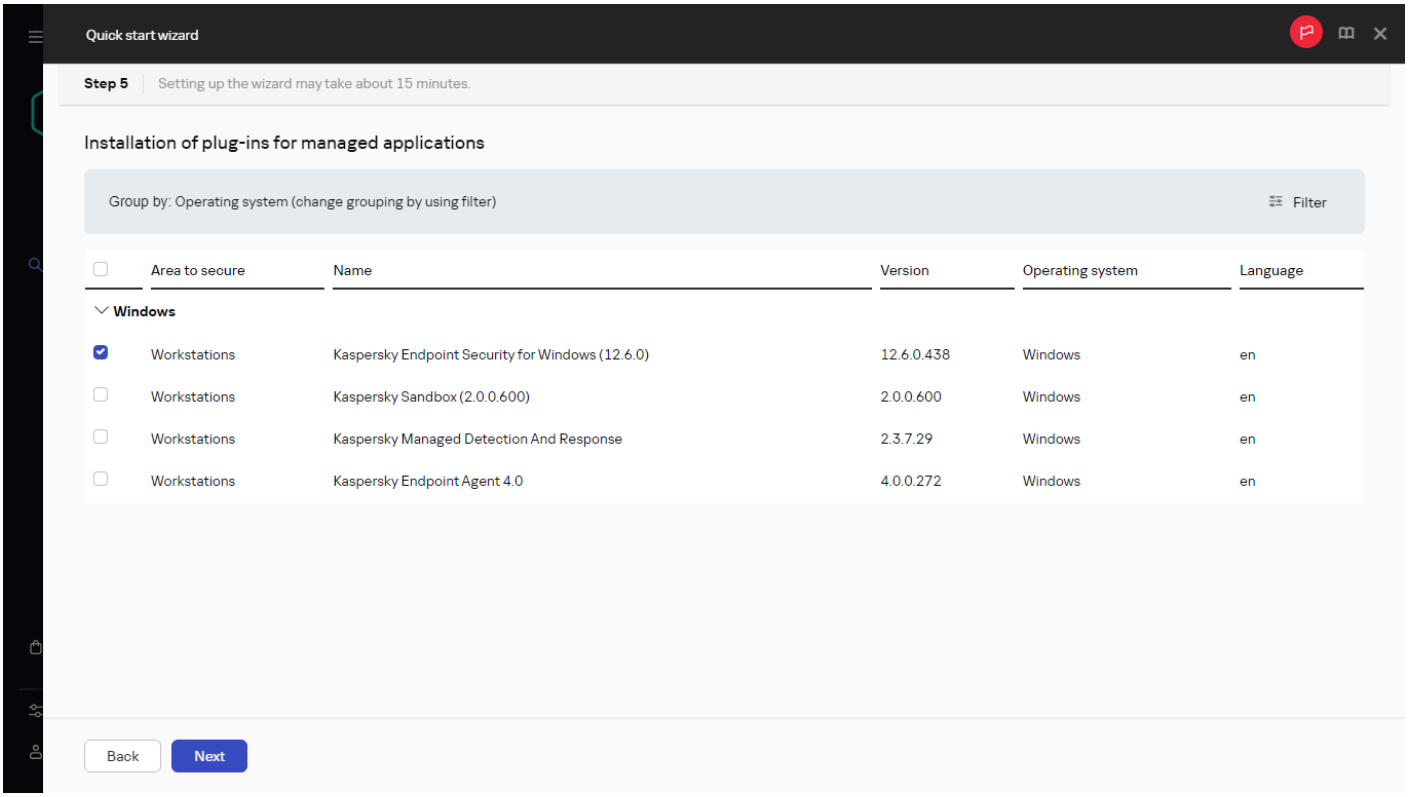
Wählen Sie im Fenster **Angebotene Verschlüsselungen** einen der folgenden Verschlüsselungs-Typen aus:

- Leichte Verschlüsselung. Dieser Verschlüsselungstyp verwendet eine 56-Bit-Schlüssellänge.
- Starke Verschlüsselung. Dieser Verschlüsselungstyp verwendet eine 256-Bit-Schlüssellänge.

Das Auswählen der Programmpakete für Kaspersky Endpoint Security für Windows mit erforderlichem Verschlüsselungstyp kann später, unabhängig vom Schnellstartassistenten, durchgeführt werden.

Schritt 5. Plug-ins für verwaltete Programme konfigurieren

Auswahl der zu installierenden Plug-ins für verwaltete Anwendungen. Eine Liste aller auf Kaspersky-Servern befindlichen Plug-ins wird angezeigt. Die Liste wird nach den Optionen gefiltert, die beim vorherigen Schritt des Assistenten ausgewählt wurden. Standardmäßig enthält eine komplette Liste Plug-ins aller Sprachen. Um nur die Plug-ins einer bestimmten Sprache anzuzeigen, nutzen Sie den Filter.



Plug-ins für verwaltete Programme installieren

Die Liste der Plug-ins umfasst die folgenden Spalten:

- **Zu schützender Bereich**

  Die ausgewählten Bereiche, die geschützt werden sollen, werden in dieser Spalte angezeigt.

- **Typ**

  In dieser Spalte werden die Plug-in-Typen angezeigt.

- **Name**

  Die Auswahl der Plug-ins richtet sich nach den Schutzbereichen und Plattformen, die Sie beim vorhergehenden Schritt ausgewählt haben.

- **Version**

  Die Liste enthält Plug-ins aller auf Kaspersky-Servern befindlichen Versionen. Standardmäßig sind die Plug-ins der aktuellsten Versionen ausgewählt.

- **Neueste Version**

  In dieser Spalte wird angezeigt, ob die Version des Plug-ins aktuell ist. Wenn der Wert **true** angezeigt wird, handelt es sich bei dem entsprechenden Plug-in um die neueste Version. Wenn der Wert **false** angezeigt wird, existiert von dem entsprechenden Plug-in eine aktuellere Version.

- **Betriebssystem**

  In dieser Spalte werden die Betriebssysteme der Plug-ins angezeigt.

- **Sprache**

  Standardmäßig wird die Lokalisierungssprache eines Plug-ins durch die Sprache von Kaspersky Security Center vorgegeben, die Sie während der Installation ausgewählt haben. In der Dropdown-Liste **Anzeige der Sprache der Verwaltungskonsole oder** können Sie andere Sprachen angeben.

Klicken Sie nach dem Auswählen der Plug-ins auf **Weiter**, um die Installation zu beginnen.

Sie können die Installation der Verwaltungs-Plug-ins für Kaspersky-Anwendungen manuell, unabhängig vom Schnellstartassistenten, durchführen.

Der Schnellstartassistent installiert die ausgewählten Plug-ins automatisch. Für die Installation einiger Plug-ins müssen Sie die Bestimmungen der EULA akzeptierten. Lesen Sie den angezeigten EULA-Text, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** und klicken Sie auf die Schaltfläche **Installieren**. Wenn Sie die Bestimmungen der EULA nicht akzeptieren, wird das Plug-in nicht installiert.

Wenn alle ausgewählten Plug-ins installiert wurden, geht der Schnellstartassistent automatisch zum nächsten Schritt über.

Schritt 6. Installieren der ausgewählten Plug-ins

Der Schnellstartassistent installiert die von Ihnen im vorherigen Schritt ausgewählten Plug-ins automatisch. Für die Installation einiger Plug-ins müssen Sie die Bestimmungen der EULA akzeptierten. Lesen Sie den angezeigten EULA-Text, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** und klicken Sie auf die Schaltfläche **Installieren**. Wenn Sie die Bestimmungen der EULA nicht akzeptieren, wird das Plug-in nicht installiert.

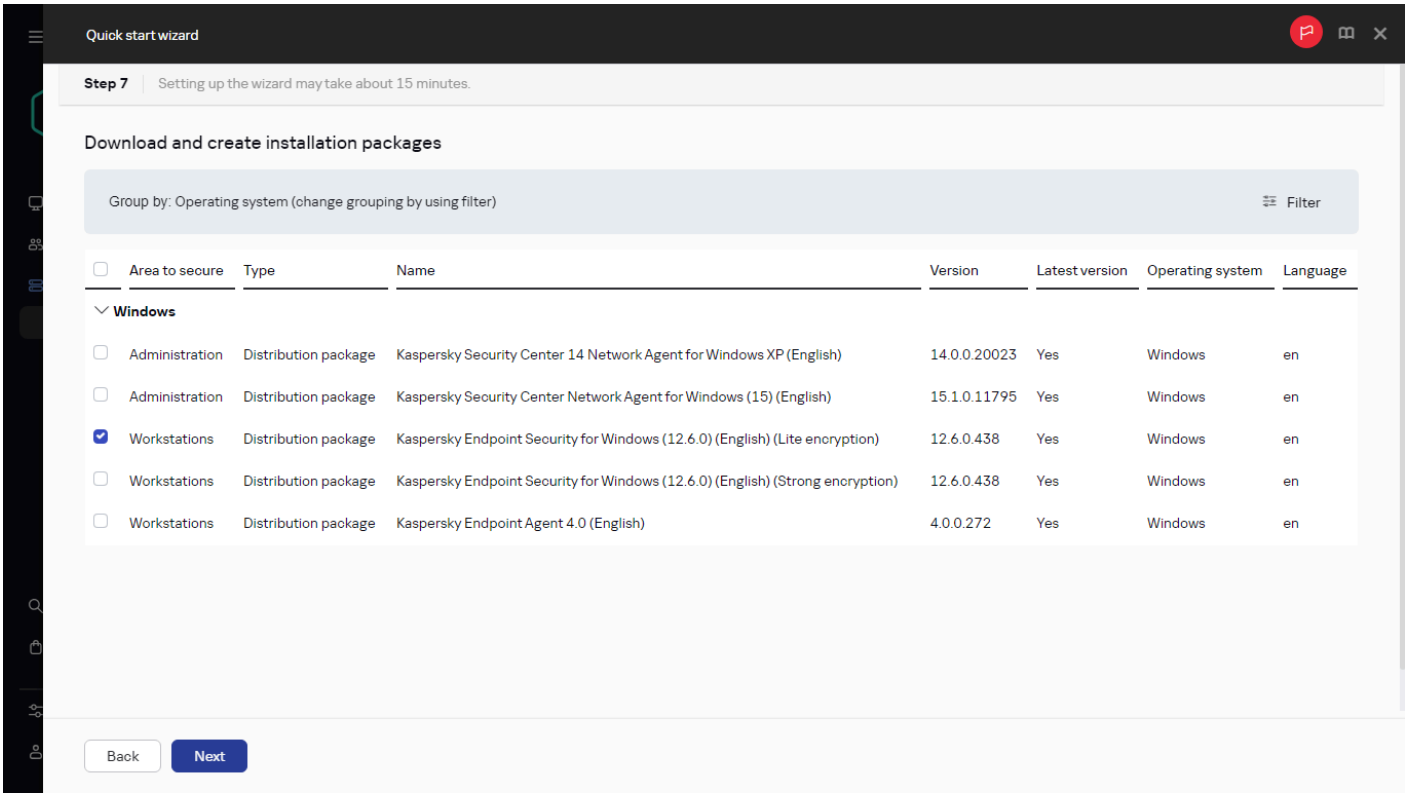
Wenn alle ausgewählten Plug-ins installiert wurden, geht der Schnellstartassistent automatisch zum nächsten Schritt über.

Schritt 7. Herunterladen der Programmpakete Erstellen der Installationspakete

Wählen Sie das herunterzuladende Programmpaket.

Für Pakete verwalteter Programme muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center installiert werden.

Nachdem Sie den Verschlüsselungstyp für Kaspersky Endpoint Security für Windows ausgewählt haben, wird eine Liste von Programmpaketen mit beiden Verschlüsselungstypen angezeigt. In der Liste ist ein Programmpaket mit dem ausgewählten Verschlüsselungstyp ausgewählt. Sie können Programmpakete eines beliebigen Verschlüsselungstyps auswählen. Die Sprache des Programmpakets entspricht der Sprache von Kaspersky Security Center. Wenn ein Programmpaket von Kaspersky Endpoint Security für Windows nicht in der Sprache von Kaspersky Security Center verfügbar ist, wird das englische Programmpaket ausgewählt.



Programmpakete herunterladen und Installationspakete erstellen

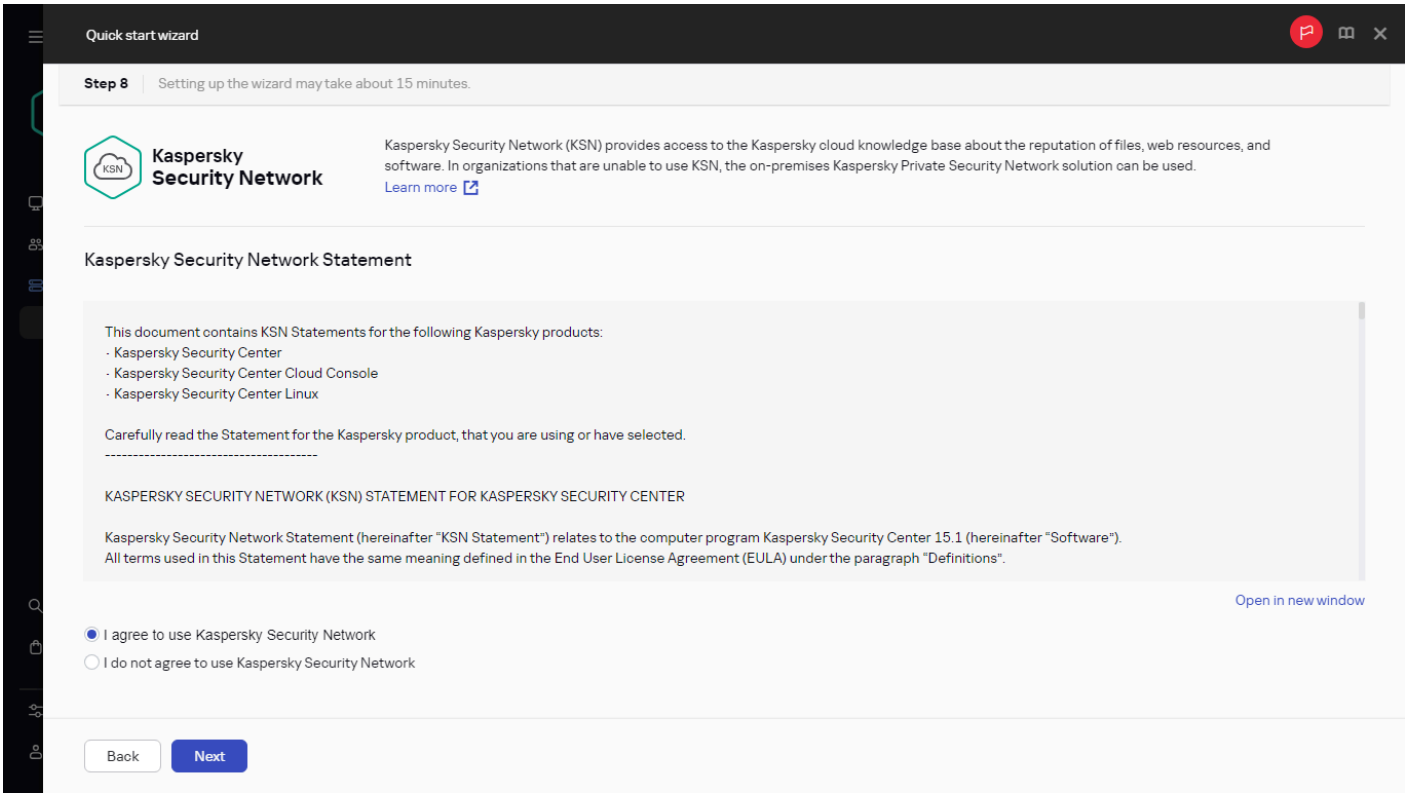
Um den Download einiger Programmpakete abzuschließen, müssen Sie die EULA akzeptieren. Wenn Sie auf die Schaltfläche **Akzeptieren** klicken, wird der EULA-Text angezeigt. Um zum nächsten Schritt des Assistenten zu wechseln, müssen Sie die Bestimmungen und Bedingungen der EULA und die Bestimmungen und Bedingungen der Kaspersky-Datenschutzrichtlinie akzeptieren. Wenn Sie die Bestimmungen und Bedingungen nicht akzeptieren, wird der Download des Pakets abgebrochen.

Nachdem Sie die Bestimmungen und Bedingungen der EULA und die Bestimmungen und Bedingungen der Kaspersky-Datenschutzrichtlinie akzeptiert haben, wird der Download des Programmpakets fortgesetzt. Die Installationspakete können Sie später verwenden, um Kaspersky-Programme auf Client-Geräten bereitzustellen.

Das Herunterladen der Programmpakete und Erstellen der Installationspakete kann später, unabhängig vom Schnellstartassistenten, durchgeführt werden.

Schritt 8. Kaspersky Security Network konfigurieren

Legen Sie die Einstellungen für die Übertragung von Informationen über die Ausführung von Kaspersky Security Center in die Wissensdatenbank von Kaspersky Security Network fest.



Kaspersky Security Network konfigurieren

Wählen Sie eine der folgenden Varianten aus:

- **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network**

  Kaspersky Security Center und die verwalteten Programme, die auf Client-Geräten installiert sind, übertragen ihre Vorgangsdetails automatisch an Kaspersky Security Network. Die Zusammenarbeit mit Kaspersky Security Network gewährleistet ein schnelleres Datenbanken-Update mit Daten über Viren und Bedrohungen, wodurch die Reaktionsgeschwindigkeit auf neue Sicherheitsgefährdungen erhöht wird.

- **Ich lehne die Nutzungsbedingungen von Kaspersky Security Network ab**

  Kaspersky Security Center und verwaltete Programme senden keine Informationen an Kaspersky Security Network.

  Wenn Sie diese Option auswählen, wird die Verwendung von Kaspersky Security Network deaktiviert.

Sie können den Zugriff auf Kaspersky Security Network (KSN) später einrichten, unabhängig vom Schnellstartassistenten.

Schritt 9. Auswählen der Methode zur Programmaktivierung

Wählen Sie eine der folgenden Varianten der Aktivierung von Kaspersky Security Center aus:

- **Durch Eingabe Ihres Aktivierungscodes**

  Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus 20 Buchstaben und Ziffern. Den Aktivierungscode geben Sie ein, um einen Schlüssel zur Aktivierung von Kaspersky Security Center hinzuzufügen. Sie erhalten den Aktivierungscode an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center angegeben haben.

  Um das Programm unter Verwendung eines Aktivierungscodes zu aktivieren, ist ein Internetzugang für die Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

  Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

  Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

  Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Knoten **Lizenzen für Kaspersky-Software** der Verwaltungskonsolenstruktur an die verwalteten Geräte verteilen.

- **Schlüsseldatei angeben**

  Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Die Schlüsseldatei dient dazu, einen Schlüssel für die Aktivierung der Anwendung hinzuzufügen.

  Die Möglichkeiten zum Abrufen einer Schlüsseldatei werden im Abschnitt Über die Schlüsseldatei beschrieben.

  Um das Programm mit einer Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

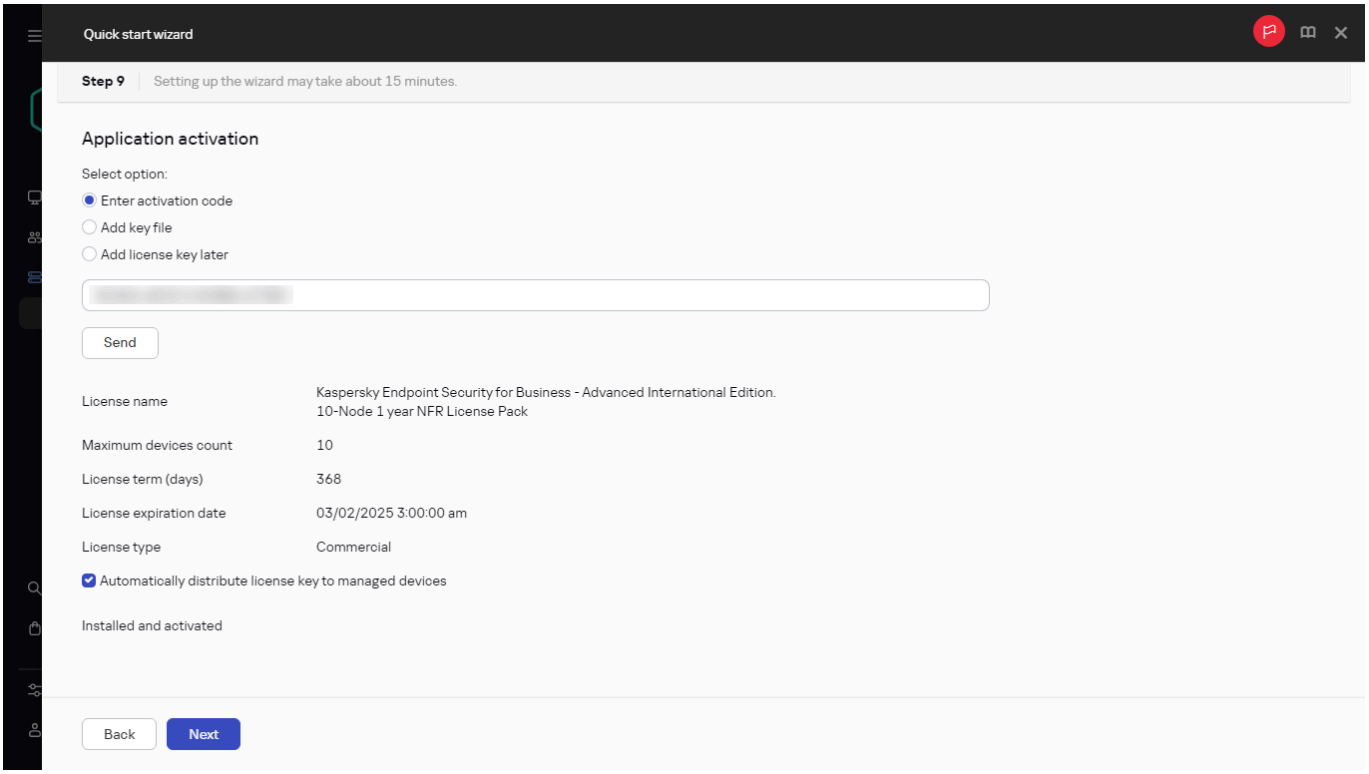
  Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

  Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

  Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Knoten **Lizenzen für Kaspersky-Software** der Verwaltungskonsolenstruktur an die verwalteten Geräte verteilen.

- **Durch ein Aufschieben der Anwendungsaktivierung**

  Das Programm wird mit grundlegenden Funktionen ausgeführt, ohne die Komponente "Verwaltung mobiler Geräte" und ohne Schwachstellen- und Patch-Management.



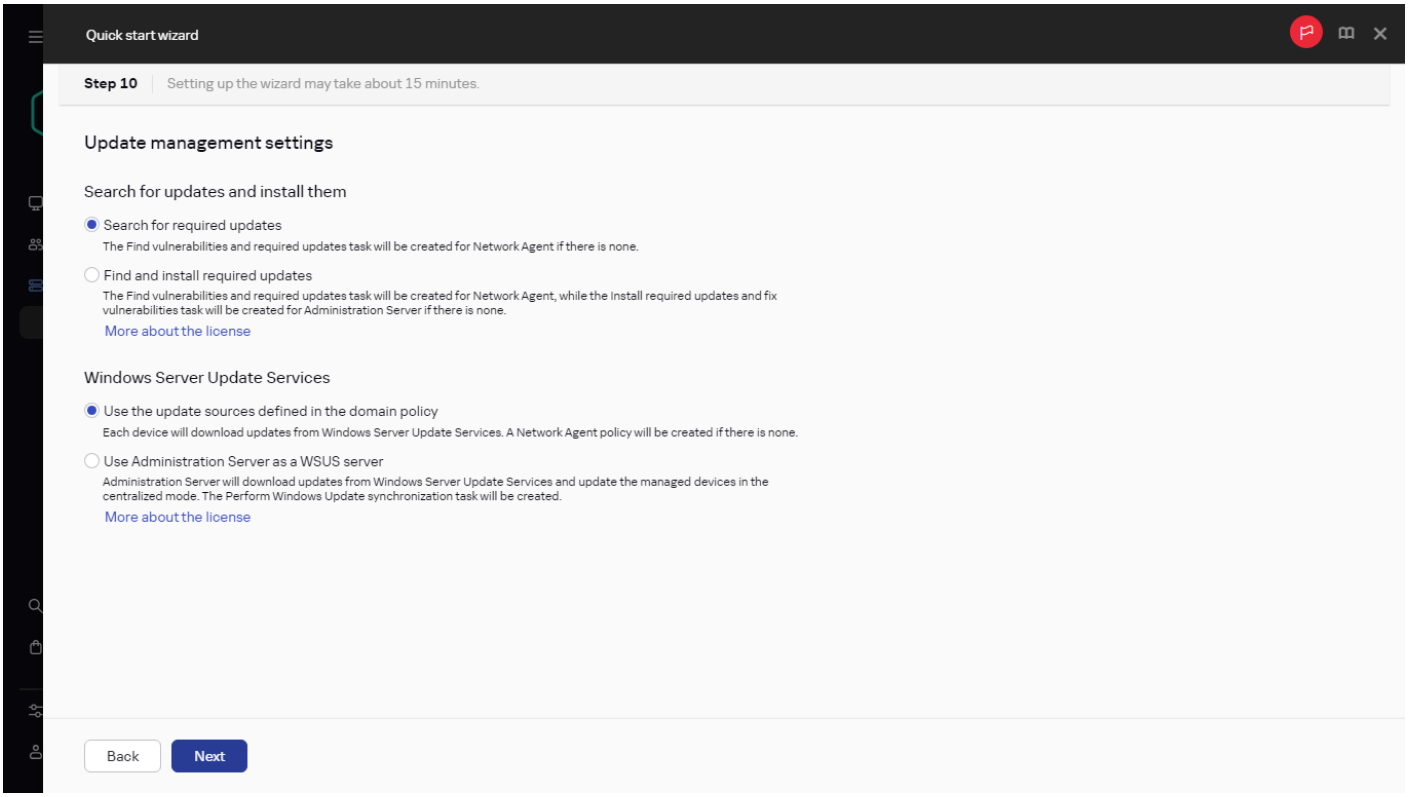
Auswählen der Methode zur Programmaktivierung

Wenn Sie die verschobene Aktivierung des Programms ausgewählt haben, können Sie den Lizenzschlüssel später jederzeit hinzufügen, indem Sie **Vorgänge** → **Lizenzierung** auswählen.

Wenn Sie mit Kaspersky Security Center aus einem gebührenpflichtigen AMI oder mit einem nutzungsbasierten, monatlich verrechneten SKU arbeiten, können Sie keine Schlüsseldateien angeben oder Aktivierungscodes eingeben.

Schritt 10. Festlegen der Einstellungen zur Verwaltung von Drittanbieter-Updates

Dieser Schritt wird nicht angezeigt, wenn Sie nicht über die Lizenz für Schwachstellen- und Patch-Management verfügen und wenn die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* bereits existiert.



Einstellungen zur Verwaltung von Drittanbieter-Updates

Wählen Sie für Updates von Drittanbieter-Programmen eine der folgenden Varianten aus:

- **Nach benötigten Updates suchen**

  Falls die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* noch nicht vorhanden ist, wird sie automatisch erstellt.

  Diese Option ist standardmäßig ausgewählt.

- **Erforderliche Updates suchen und installieren**

  Die Aufgaben *Suche nach Schwachstellen und erforderlichen Updates* und *Erforderliche Updates installieren und Schwachstellen schließen* werden automatisch erstellt, sofern sie noch nicht vorhanden sind.

  Diese Variante ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Wählen Sie für Updates von Windows Updates eine der folgenden Varianten aus:

- **Die in der Domänenrichtlinie angegeben Update-Quellen verwenden**

  Die Client-Geräte laden Windows-Updates in Übereinstimmung mit den Einstellungen Ihrer Domänenrichtlinie herunter. Die Richtlinie des Administrationsagenten wird automatisch erstellt, sofern sie noch nicht vorhanden ist.

- **Administrationsserver als WSUS-Server verwenden**

  Die Client-Geräte laden Windows-Updates vom Administrationsserver herunter. Die Aufgabe *Windows-Updates synchronisieren* und die Richtlinie des Administrationsagenten werden automatisch erstellt, sofern sie noch nicht vorhanden sind.

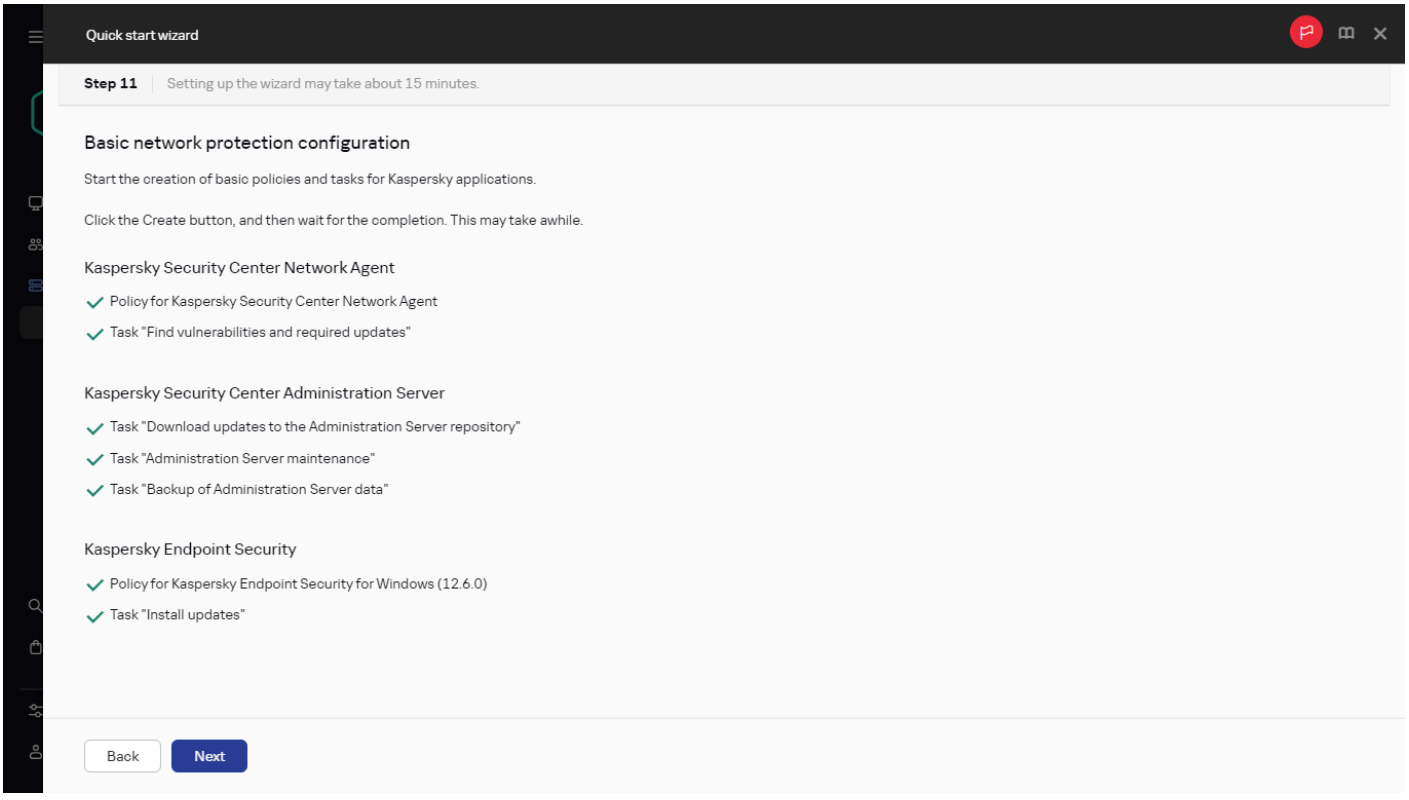
  Diese Variante ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Sie können die Aufgaben *Suche nach Schwachstellen und erforderlichen Updates* und *Erforderliche Updates installieren und Schwachstellen schließen* separat vom Schnellstartassistenten erstellen. Um den Administrationsserver als WSUS-Server zu verwenden, erstellen Sie die Aufgabe *Windows-Updates synchronisieren* und wählen Sie anschließend in der Richtlinie des Administrationsagenten die Option **Administrationsserver als WSUS-Server verwenden**.

Schritt 11. Erstellen einer grundlegenden Konfiguration für Netzwerkschutz

Sie können die Liste mit Richtlinien und Aufgaben, die erstellt werden, überprüfen.

Bevor Sie zum nächsten Schritt des Assistenten wechseln können, müssen Sie warten, bis die Erstellung der Richtlinien und Aufgaben abgeschlossen ist.

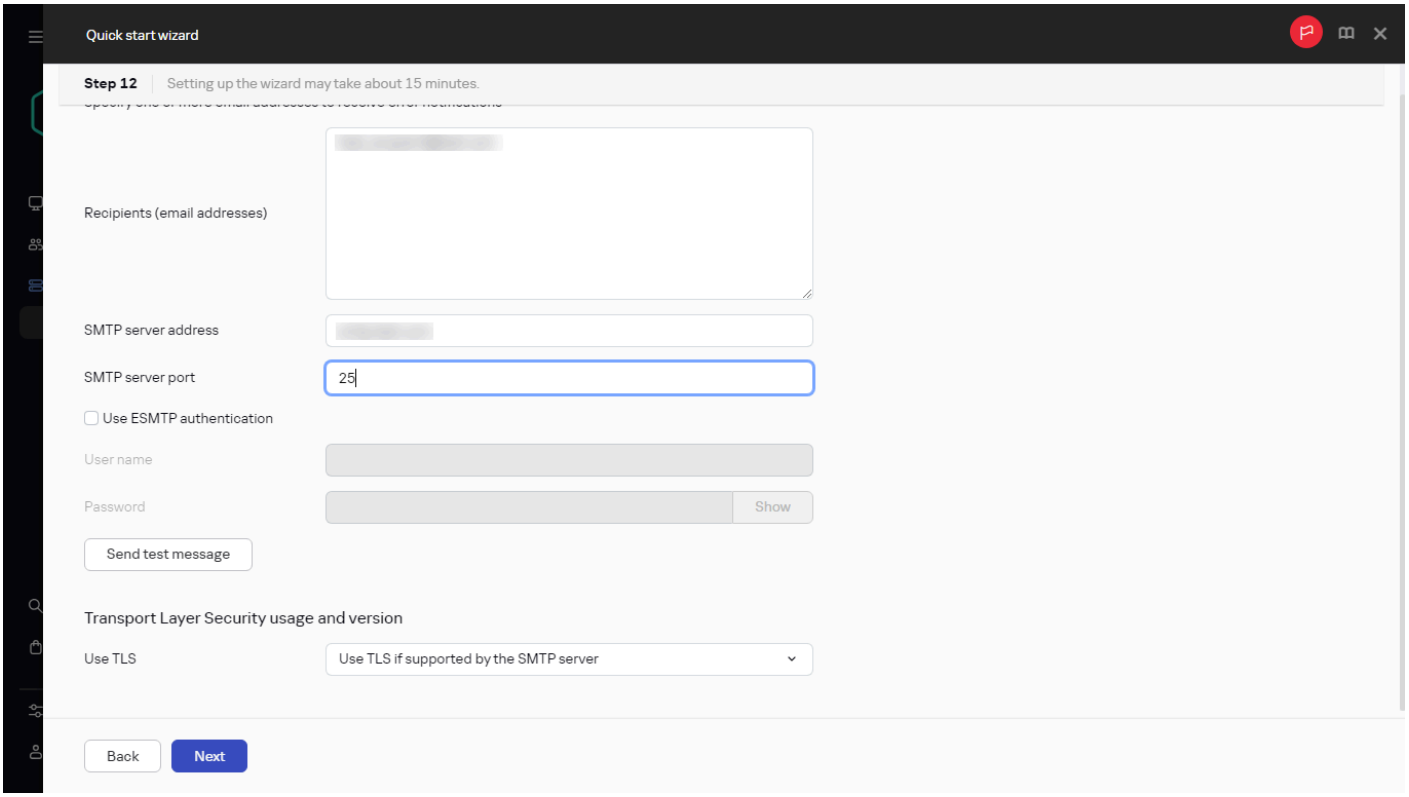


Erstellen einer grundlegenden Konfiguration für Netzwerkschutz

Sie können die erforderlichen Aufgaben und Richtlinien später erstellen, unabhängig vom Schnellstartassistenten.

Schritt 12. Konfigurieren von E-Mail-Benachrichtigungen

Passen Sie die Einstellungen für den Versand von Benachrichtigungen über Ereignisse an, die bei der Ausführung von Kaspersky-Anwendungen auf den Client-Geräten registriert werden. Diese Einstellungen werden in den Richtlinien für die Anwendungen als Standardwerte verwendet.



Konfigurieren von E-Mail-Benachrichtigungen

Folgende Einstellungen für den Versand von Benachrichtigungen über auftretende Ereignisse der Kaspersky-Anwendungen können angepasst werden:

- **Empfänger (E-Mail-Adressen)**

  E-Mail-Adressen des Nutzers, an welche die Anwendung Benachrichtigungen versenden soll. Sie können eine oder mehrere Adressen angeben. Geben Sie mehrere Adressen durch Semikolon getrennt an.

- **Adresse des SMTP-Servers**

  Adresse oder Adressen der Mail-Server Ihres Unternehmens.

  Geben Sie mehrere Adressen durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

  - IPv4- oder IPv6-Adresse
  - Windows-Netzwerkname (NetBIOS-Name) des Geräts
  - DNS-Name des SMTP-Servers

- **Port des SMTP-Servers**

  Kommunikationsportnummer des SMTP-Servers Wenn Sie mehrere SMTP-Server verwenden, wird die Verbindung zu diesen über den angegebenen Kommunikationsport hergestellt. Standardmäßig wird Portnummer 25 verwendet.

- **ESMTP-Authentifizierung verwenden**

  Aktivierung der Unterstützung von ESMTP-Authentifizierung. Nach der Aktivierung des Kontrollkästchens in den Feldern **Benutzername** und **Kennwort** können die Einstellungen für ESMTP-Authentifizierung angeben werden. Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **TLS verwenden**

  Sie können die TLS-Einstellungen einer Verbindung mit einem SMTP-Server angeben:

  - **TLS nicht verwenden**

    Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

  - **TLS verwenden, wenn dies vom SMTP-Server unterstützt wird**

    Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

  - **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen**

    Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

    > Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

    Wenn Sie den Wert **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen** ausgewählt haben, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

  Sie können Zertifikate für eine TLS-Verbindung angeben, indem Sie auf den Link **Zertifikate angeben** klicken:

  - Geben Sie eine Datei mit SMTP-Server-Zertifikat an:

    Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center prüft, ob das Zertifikat eines SMTP-Servers auch von eine vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

  - Geben Sie die Datei des Client-Zertifikats an:

    Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen Zertifizierungsstelle. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

    - X-509-Zertifikat:

      Sie müssen eine Datei mit dem Zertifikat und eine Datei mit dem privaten Schlüssel angeben. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Laden der Dateien ist spielt keine Rolle. Wenn beide Dateien geladen sind, müssen Sie das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- pkcs12-Container:

  Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

Sie können die festgelegten Versandeinstellungen der E-Mail-Benachrichtigungen mithilfe der Schaltfläche **Testnachricht senden** prüfen.

Sie können die Ereignisbenachrichtigungen später konfigurieren, unabhängig vom Schnellstartassistenten.

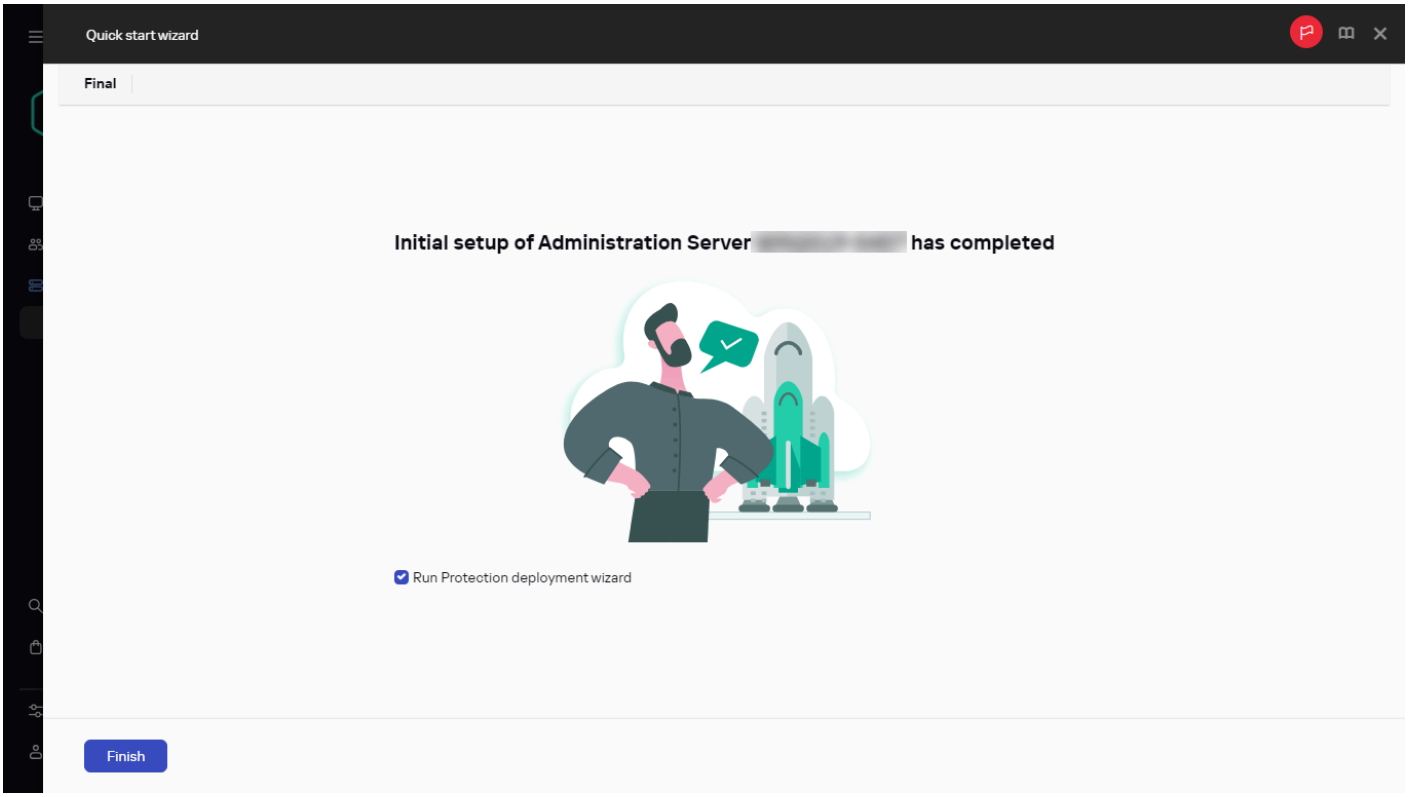
Schritt 13. Durchführen einer Netzwerkabfrage

Der Administrationsserver führt eine erste Abfrage aus. Während der Abfrage wird eine Fortschrittsleiste angezeigt. Nach Abschluss der Abfrage wird der Link **Erkannte Geräte anzeigen** verfügbar. Klicken Sie auf diesen Link, um die Netzwerkgeräte anzuzeigen, die der Administrationsserver gefunden hat. Drücken Sie die **Escape**-Taste, um zum Schnellstartassistenten zurückzukehren.

Sie können Ihr Netzwerk später, unabhängig vom Schnellstartassistenten, abfragen. Verwenden Sie die Kaspersky Security Center Web Console, um das Abfragen eines Domänen-Controllers, von Windows-Domänen, IP-Bereichen und IPv6-Netzwerkes zu konfigurieren.

Schritt 14. Abschließen des Schnellstartassistenten

Aktivieren Sie auf der letzten Seite des Schnellstartassistenten das Kontrollkästchen **Assistent für die Bereitstellung des Schutzes starten**, wenn Sie die automatische Installation der Antiviren-Programme oder des Administrationsagenten auf den Geräten in Ihrem Netzwerk starten möchten.



Abschließender Schritt des Schnellstartassistenten

Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

Verbinden mobiler Geräte

Dieser Abschnitt beschreibt, wie Sie mobile Geräte (d.h. verwaltete Geräte, die sich außerhalb des Hauptnetzwerks befinden) mit dem Administrationsserver verbinden.

Szenario: Verbinden von mobilen Geräten mittels Verbindungs-Gateway

Dieses Szenario beschreibt, wie Sie verwaltete Geräte, die sich außerhalb des Hauptnetzwerks befinden, mit dem Administrationsserver verbinden.

Erforderliche Vorrausetzungen

Für dieses Szenario müssen die folgenden Voraussetzungen erfüllt sein:

- Eine demilitarisierte Zone (DMZ) ist im Netzwerk Ihrer Organisation eingerichtet.
- Ein Kaspersky Security Center Administrationsserver ist im Unternehmensnetzwerk bereitgestellt.

Schritte

Das Szenario verläuft in Stufen:

1. **Auswählen eines Client-Gerätes innerhalb der DMZ**

   Das Gerät wird als Verbindungs-Gateway verwendet. Das von Ihnen ausgewählte Gerät muss den Anforderungen an ein Verbindungs-Gateway entsprechen.

2. **Installation des Administrationsagenten für seine Rolle als Verbindungs-Gateway**

   Für die Installation des Administrationsagenten auf dem ausgewählten Gerät wird eine lokale Installation empfohlen.

   Standardmäßig befindet sich die Installationsdatei unter: \\<Servername>\KLSHARE\PkgInst\NetAgent_<Versionsnummer>

   Wählen Sie im Installationsassistenten des Administrationsagenten im Fenster **Verbindungs-Gateway** die Option **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden**. Dieser Modus aktiviert die Rolle als Verbindungs-Gateway und unterweist gleichzeitig den Administrationsagenten, auf Verbindungen vom Administrationsserver zu warten, anstelle Verbindungen zum Administrationsserver herzustellen.

   Alternativ können Sie den Administrationsagent auf einem Linux-Gerät installieren und so konfigurieren, dass er als Verbindungs-Gateway fungiert, sollten dabei aber die Liste der Einschränkungen von Administrationsagenten auf Linux-Geräten beachten.

3. **Erlauben von Verbindungen in den Firewalls auf dem Verbindungs-Gateway**

   Um sicherzustellen, dass sich der Administrationsserver tatsächlich mit dem Verbindungs-Gateway in der DMZ verbinden kann, erlauben Sie Verbindungen zu TCP-Port 13000 in allen Firewalls zwischen dem Administrationsserver und dem Verbindungsgateway.

   Wenn das Verbindungs-Gateway keine echte IP-Adresse im Internet besitzt, sich aber stattdessen hinter einer Network Address Translation (NAT) befindet, konfigurieren Sie eine Regel für das Forwarding von Verbindungen über NAT.

4 Erstellen einer Administrationsgruppe für externe Geräte

Erstellen Sie eine neue Gruppe unter der Gruppe **Verwaltete Geräte**. Diese neue Gruppe wird die externen verwalteten Geräte enthalten.

5 Verbinden des Verbindungs-Gateways mit dem Administrationsserver

Das von Ihnen konfigurierte Verbindungs-Gateway wartet auf eine Verbindung vom Administrationsserver. Der Administrationsserver zeigt das Gerät mit dem Verbindungs-Gateway jedoch nicht unter den verwalteten Geräten an. Das liegt daran, dass das Verbindungs-Gateway noch nicht versucht hat, eine Verbindung mit dem Administrationsserver herzustellen. Es ist daher eine spezielle Vorgehensweise notwendig, um sicherzustellen, dass der Administrationsserver eine Verbindung zum Verbindungs-Gateway initiiert.

Führen Sie folgende Schritte aus:

1. Fügen Sie das Verbindungs-Gateway als Verteilungspunkt hinzu.
2. Verschieben Sie das Verbindungs-Gateway von der Gruppe **Nicht zugeordnete Geräte** in die Gruppe, die Sie für externe Geräte angelegt haben.

Das Verbindungs-Gateway ist verbunden und konfiguriert.

6 Verbinden von externen Desktop-Geräten mit dem Administrationsserver

In der Regel werden externe Desktop-Geräte nicht in den Perimeter hinein bewegt. Daher müssen Sie die Geräte während der Installation des Administrationsagenten so konfigurieren, dass sie sich über das Verbindungs-Gateway mit dem Administrationsserver verbinden.

7 Konfigurieren von Updates für externe Desktop-Geräte

Wenn die Updates der Sicherheitsanwendungen so konfiguriert sind, dass sie vom Administrationsserver heruntergeladen werden, laden sich externe Geräte die Updates über das Verbindungs-Gateway herunter. Das hat zwei Nachteile:

- Es entsteht unnötiger Traffic, welcher Bandbreite vom Internet-Kommunikationskanal des Unternehmens in Beschlag nimmt.
- Es ist nicht zwangsläufig die schnellste Art, Updates zu beziehen. Es ist anzunehmen, dass es für externe Geräte günstiger und schneller wäre, ihre Updates von Kaspersky-Update-Servern zu beziehen.

Führen Sie folgende Schritte aus:

1. Verschieben Sie alle externen Geräte in die separate Administrationsgruppe, die Sie zu einem früheren Zeitpunkt angelegt haben.
2. Schließen Sie die Gruppe mit den externen Geräten von der Update-Aufgabe aus.
3. Erstellen Sie eine separate Update-Aufgabe für die Gruppe mit den externen Geräten.

8 Verbinden von Laptops, die Reisetätigkeiten unterliegen, mit dem Administrationsserver

Reiselaptops befinden sich manchmal innerhalb und manchmal außerhalb des Netzwerks. Um deren Verwaltung effizient zu gestalten, müssen sich diese Geräte, abhängig von deren Standort, auf unterschiedliche Weise mit dem Administrationsserver verbinden. Für effizienten Traffic müssen die Geräte ebenfalls in Abhängigkeit von ihrem Standort Updates aus verschiedenen Quellen beziehen.

Sie müssen Regeln für mobile Benutzer konfigurieren: Verbindungsprofile und Beschreibungen der Standorte im Netzwerk. Jede Regel gibt an, mit welcher Instanz eines Administrationsservers sich die Reiselaptops in Abhängigkeit ihres Standortes verbinden müssen und von welcher Instanz eines Administrationsservers sie ihre Updates beziehen müssen.

Szenario: Verbinden von mobilen Geräten mittels einem sekundären Administrationsserver in der DMZ

Wenn Sie mit dem Administrationsserver verwaltete Geräte verbinden möchten, die sich außerhalb des Hauptnetzwerks befinden, können Sie einen sekundären Administrationsserver verwenden, der sich in der demilitarisierten Zone (DMZ) befindet.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

- Im Netzwerk Ihrer Organisation ist eine DMZ eingerichtet.
- Kaspersky Security Center Administrationsserver wurde im internen Unternehmensnetzwerk bereitgestellt.

Schritte

Das Szenario verläuft in Stufen:

1. **Auswählen eines Client-Gerätes innerhalb der DMZ**

   Wählen Sie in der DMZ ein Client-Gerät aus, das als sekundärer Administrationsserver verwendet werden soll.

2. **Kaspersky Security Center Administrationsserver installieren**

   Installation von Kaspersky Security Center Administrationsserver auf diesem Client-Gerät.

3. **Eine Administrationsserver-Hierarchie erstellen**

   Wenn Sie einen sekundären Administrationsserver in der DMZ platzieren, muss der sekundäre Administrationsserver eine Verbindung vom primären Administrationsserver annehmen können. Fügen Sie dafür einen neuen Administrationsserver als sekundär hinzu, damit sich der primäre Administrationsserver über Port 13000 mit dem sekundären Administrationsserver verbindet. Bei der Zusammenfassung der Administrationsserver in der Hierarchie ist es erforderlich, dass der Port 13299 beider Server verfügbar ist. Die Kaspersky Security Center Web Console verbindet sich mit einem Administrationsserver über den SSL-Port TCP 13299.

4. **Verwaltete mobile Geräte mit dem sekundären Administrationsserver verbinden**

   Sie können mobile Geräte auf die gleiche Weise mit dem Administrationsserver in der DMZ verbinden, wie beim Verbindungsaufbau zwischen dem Administrationsserver und den verwalteten Geräten, die sich im Hauptnetzwerk befinden. Verwaltete mobile Geräten initiieren die Verbindung über Port 13000.

Über das Verbinden mobiler Geräte

Einige verwaltete Geräte befinden sich dauerhaft außerhalb des Hauptnetzwerks (z. B. Geräte in regionalen Unternehmensniederlassungen, Kiosks, Geldautomaten, an verschiedenen Point-of-Sales installierte Terminals, Geräte im Home-Office von Angestellten). Einige Geräte bewegen sich von Zeit zu Zeit außerhalb des Perimeters (z. B. Laptops von Benutzern, die regionale Niederlassungen oder das Büro eines Kunden besuchen).

Auch von solchen mobilen Geräten muss der Schutz überwacht und verwaltet werden, d. h. es muss möglich sein, aktuelle Informationen über den Schutzstatus der Geräte abzurufen und die auf ihnen installierten Sicherheitsanwendungen aktuell zu halten. Dies ist beispielsweise wichtig für den Fall, in dem ein solches Gerät kompromittiert wird, während es sich außerhalb des Hauptnetzwerks befindet. In der Folge kann das Gerät beim erneuten Verbinden mit dem Hauptnetzwerk zu einer Plattform sich ausbreitender Bedrohungen werden. Sie können zwei Methoden verwenden, um mobile Geräte mit dem Administrationsserver zu verbinden:

- Verbindungs-Gateway in der demilitarisierten Zone (DMZ)

  Schema des Datenverkehrs: Administrationsserver im LAN, verwaltete Geräte im Internet, Verbindungs-Gateway wird verwendet.

- Administrationsserver in der DMZ

  Schema des Datenverkehrs: Administrationsserver in DMZ, verwaltete Geräte im Internet

Ein Verbindungs-Gateway in der DMZ

Eine empfohlene Methode zum Verbinden von mobilen Geräten mit dem Administrationsserver besteht darin, eine DMZ im Netzwerk des Unternehmens zu organisieren und ein Verbindung-Gateway in der DMZ zu installieren. Externe Geräte verbinden sich mit dem Verbindungs-Gateway und der Administrationsserver innerhalb des Netzwerks initiiert die Verbindung zu den Geräten über das Verbindungs-Gateway.

Im Vergleich zu der anderen Methode ist diese sicherer:

- Sie müssen den Zugriff auf den Administrationsserver nicht von außerhalb des Netzwerks öffnen.
- Ein kompromittiertes Verbindungs-Gateway stellt kein hohes Risiko für die Sicherheit der Netzwerkgeräte dar. Ein Verbindungs-Gateway verwaltet im Grunde nichts selbst und stellt keine Verbindungen her.

Außerdem erfordert ein Verbindungs-Gateway nicht viele Hardware-Ressourcen.

Der Konfigurationsprozess dieser Methode ist jedoch komplexer:

- Damit ein Gerät als Verbindungs-Gateway in der DMZ fungiert, müssen Sie den Administrationsagenten installieren und auf eine bestimmte Weise mit dem Administrationsserver verbinden.
- Sie können nicht in allen Situationen dieselbe Adresse für die Verbindung zum Administrationsserver verwenden. Von außerhalb des Perimeters müssen Sie nicht nur eine andere Adresse verwenden (Adresse des Verbindungs-Gateways), sondern auch einen anderen Verbindungsmodus (über ein Verbindungs-Gateway).
- Sie müssen auch unterschiedliche Verbindungseinstellungen für Laptops an verschiedenen Standorten festlegen.

So fügen Sie einem zuvor konfigurierten Netzwerk ein Verbindungs-Gateway hinzu:

1. Installieren Sie Administrationsagenten Verbindungs-Gateway-Modus.
2. Installieren Sie den Administrationsagenten auf den Geräten erneut, die Sie mit dem neu hinzugefügten Verbindungs-Gateway verbinden möchten.

Administrationsserver in der DMZ

Eine andere Methode ist die Installation eines einzelnen Administrationsservers in der DMZ.

Diese Konfiguration ist weniger sicher als die andere Methode. Um in diesem Fall externe Laptops zu verwalten, muss der Administrationsserver Verbindungen von jeder Adresse im Internet akzeptieren. Es werden weiterhin alle Geräte im internen Netzwerk verwaltet, jedoch erfolgt dies aus der DMZ. Daher kann ein kompromittierter Server trotz der geringen Wahrscheinlichkeit eines solchen Ereignisses einen enormen Schaden verursachen.

Das Risiko wird erheblich geringer, wenn der Administrationsserver in der DMZ keine Geräte im internen Netzwerk verwaltet. Eine solche Konfiguration kann beispielsweise von einem Dienstanbieter verwendet werden, um die Geräte von Kunden zu verwalten.

Möglicherweise möchten Sie diese Methode in den folgenden Fällen verwenden:

- Wenn Sie mit der Installation und Konfiguration des Administrationsservers vertraut sind und kein anderes Verfahren zum Installieren und Konfigurieren eines Verbindungsgateways ausführen möchten.
- Wenn Sie mehr Geräte verwalten müssen. Die maximale Kapazität der Administrationsserver beträgt 100.000 Geräte, während ein Verbindungs-Gateway bis zu 10.000 Geräte unterstützen kann.

Auch diese Lösung birgt mögliche Schwierigkeiten:

- Der Administrationsserver benötigt mehr Hardware-Ressourcen und eine zusätzliche Datenbank.
- Informationen zu Geräten werden in zwei unabhängigen Datenbanken gespeichert (für Administrationsserver im Netzwerk und eine weitere in der DMZ), was die Überwachung erschwert.
- Um alle Geräte zu verwalten, muss der Administrationsserver zu einer Hierarchie zusammengefügt werden, was nicht nur die Überwachung, sondern auch die Verwaltung erschwert. Eine Instanz eines sekundären Administrationsservers schränkt die möglichen Strukturen von Administrationsgruppen ein. Sie müssen entscheiden, wie und welche Aufgaben und Richtlinien an eine Instanz eines sekundären Administrationsservers verteilt werden sollen.
- Das Konfigurieren externer Geräte zur Verwendung des Administrationsservers in der DMZ von außen und zur Verwendung des primären Administrationsservers von innen ist komplexer, als sie nur für die Verwendung einer bedingten Verbindung über ein Gateway zu konfigurieren.
- Hohe Sicherheitsrisiken. Eine kompromittierte Instanz eines Administrationsservers erleichtert die Kompromittierung der von ihr verwalteten Laptops. In diesem Fall müssen die Hacker nur warten, bis einer der Laptops zum Unternehmensnetzwerk zurückkehrt, damit sie ihren Angriff auf das lokale Netzwerk fortsetzen können.

Verbinden von externen Desktop-Geräten mit dem Administrationsserver

Geräte, die sich dauerhaft außerhalb des Hauptnetzwerks befinden (z. B. Geräte in regionalen Unternehmensniederlassungen, Kiosks, Geldautomaten, an verschiedenen Point-of-Sales installierte Terminals, Geräte im Home-Office von Angestellten) können nicht direkt mit dem Administrationsserver verbunden werden. Stattdessen müssen sie mit dem Administrationsserver über einen Verbindungs-Gateway verbunden werden, welches in der demilitarisierten Zone (DMZ) platziert ist. Die dafür notwendige Konfiguration wird vorgenommen, wenn der Administrationsagent auf diesen Geräten installiert wird.

Um externe Desktop-Geräte mit dem Administrationsserver zu verbinden:

1. Erstellen ein neues Installationspaket für den Administrationsagenten.
2. Öffnen Sie die Eigenschaften des erstellten Installationspakets, wechseln Sie zum Abschnitt **Einstellungen** → **Erweitert** und wählen Sie anschließend die Option **Eine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen**.

   Die Einstellung **Eine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen** ist inkompatibel zur Einstellung **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden**. Beide Einstellungen können nicht gleichzeitig aktiv sein.

3. Geben Sie im Feld **Adresse des Verbindungs-Gateways** die öffentliche Adresse des Verbindungs-Gateways an.

   Wenn sich der Verbindungs-Gateway hinter einer Network Address Translation (NAT) befindet und keine eigene öffentliche Adresse besitzt, konfigurieren Sie eine NAT-Gateway-Regel für das Forwarding von Verbindungen aus öffentlichen Adressen zur internen Adresse des Verbindungs-Gateways.

4. Erstellen Sie ein autonomes Installationspaket auf Grundlage des erstellten Installationspakets.
5. Übermitteln Sie das autonome Installationspaket entweder elektronisch oder mithilfe eines Wechseldatenträgers an das Zielgerät.
6. Installieren Sie den Administrationsagenten aus dem autonomes Paket.

Die externen Geräte sind mit dem Administrationsserver verbunden.

Über Verbindungsprofile für mobile Benutzer

Bei der Arbeit der mobilen Benutzer, die Laptops (im Weiteren auch "Geräte") verwenden, kann es erforderlich sein, die Verbindungsmethode mit dem Administrationsserver zu ändern oder abhängig von aktuellen Standort des Geräts im Netzwerk zwischen Administrationsservern umzuschalten.

Verbindungsprofile werden nur für Geräte mir Windows oder macOS unterstützt.

Nutzung verschiedener Adressen ein- und desselben Administrationsservers

Die Geräte mit installiertem Administrationsagenten können in unterschiedlichen Zeiträumen sowohl aus dem internen Netzwerk des Unternehmens als auch aus dem Internet mit dem Administrationsserver verbunden werden. In dieser Situation kann es erforderlich sein, dass der Administrationsagent verschiedene Adressen für die Verbindung mit dem Administrationsserver verwendet: die externe Adresse des Servers bei der Verbindung aus dem Internet und die interne Adresse des Servers bei der Verbindung aus dem internen Netzwerk.

Fügen Sie daher in den Eigenschaften der Richtlinie des Administrationsagenten ein Profil für die Verbindung zum Administrationsserver über das Internet hinzu (im Abschnitt **Programmeinstellungen → Konnektivität → Verbindungsprofile → Verbindungsprofile des Administrationsservers**). Deaktivieren Sie im Fenster für die Profilerstellung die Option **Nur für Update-Download verwenden** und stellen Sie sicher, dass die Option **Verbindungseinstellungen mit den in diesem Profil angegeben Einstellungen des Administrationsservers synchronisieren** ausgewählt ist. Wenn für den Zugriff auf den Administrationsserver ein Verbindungs-Gateway verwendet wird (beispielsweise in einer Konfiguration von Kaspersky Security Center vom Typ Zugriff aus dem Internet: Administrationsagent als Verbindungs-Gateway in der demilitarisierten Zone), muss im Verbindungsprofil die Adresse des Verbindungs-Gateways im entsprechenden Feld angegeben werden.

Umschaltung zwischen Administrationsservern in Abhängigkeit vom aktuellen Netzwerk

Wenn es im Unternehmen mehrere Büros mit verschiedenen Administrationsservern gibt und zwischen ihnen ein Teil der Geräte mit installiertem Administrationsagenten verschoben wird, ist es erforderlich, dass der Administrationsagent mit dem Administrationsserver des lokalen Netzwerkes jenes Büros verbunden wird, in dem sich das Gerät befindet.

Erstellen Sie in diesem Fall in den Eigenschaften der Richtlinie des Administrationsagenten ein Profil für Verbindung mit Administrationsserver für jedes der Büros, mit Ausnahme des Büros, in dem sich der Home-Administrationsserver befindet. Geben Sie in den Verbindungsprofilen die Adressen der entsprechenden Administrationsserver an und aktivieren oder deaktivieren Sie die Option **Nur für Update-Download verwenden**:

- Aktivieren Sie die Option, wenn es erforderlich ist, dass sich der Administrationsagent mit dem Home-Administrationsserver synchronisiert und der lokale Server nur für den Update-Download verwendet wird.
- Deaktivieren Sie diese Option, wenn erforderlich ist, dass der Administrationsagent den lokalen Administrationsserver vollständig verwaltet.

Des Weiteren müssen die Bedingungen für die Umschaltung auf die erstellten Profile angepasst werden: mindestens eine Bedingung für jedes Büro, mit Ausnahme des "Home-Office". Der Sinn jeder solchen Bedingung besteht in der Sichtbarkeit der büroeigenen Details in der Netzwerkumgebung. Wenn eine Bedingung erfüllt wird, erfolgt die Aktivierung des entsprechenden Profils. Trifft keine der Bedingungen zu, wird der Administrationsagent auf den Home-Administrationsserver umgeschaltet.

Erstellen eines Verbindungsprofils für mobile Benutzer

Ein Profil zur Verbindung mit dem Administrationsserver steht nur auf Geräten mit Windows oder macOS zur Verfügung.

Um für mobile Benutzer ein Profil für die Verbindung des Administrationsagenten zum Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Wenn Sie ein Verbindungsprofil für eine Gruppe verwalteter Geräte erstellen möchten, öffnen Sie die Richtlinie des Administrationsagenten dieser Gruppe. Gehen Sie dafür folgendermaßen vor:

   a. Wechseln Sie im Hauptmenü zu **Assets (Geräte) → Richtlinien und Profile**.

   b. Klicken Sie auf den Link des aktuellen Pfads.

c. Wählen Sie im sich öffnenden Fenster die erforderliche Administrationsgruppe aus.

Anschließend wird der aktuelle Pfad geändert.

d. Fügen Sie die Richtlinie des Administrationsagenten für die Gruppe der verwalteten Geräte hinzu. Wenn Sie diese bereits erstellt haben, klicken Sie auf den Namen der Richtlinie des Administrationsagenten, um ihre Eigenschaften zu öffnen.

2. Wenn Sie ein Verbindungsprofil für ein bestimmtes verwaltetes Gerät erstellen möchten, gehen Sie wie folgt vor:

a. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

b. Klicken Sie auf den Namen des verwalteten Geräts.

c. Wechseln Sie im sich öffnenden Eigenschaftenfenster des verwalteten Geräts auf die Registerkarte **Programme**.

d. Klicken Sie auf den Namen der Richtlinie des Administrationsagenten, für die nur das ausgewählte verwaltete Gerät gilt.

3. Wechseln Sie im sich öffnenden Eigenschaftenfenster zu **Programmeinstellungen** → **Konnektivität** → **Verbindungsprofile.**

4. Klicken Sie im Abschnitt **Verbindungsprofile des Administrationsservers** auf **Hinzufügen**.

Standardmäßig enthält die Liste der Verbindungsprofile die Profile <Autonomer-Modus> und <Home-Administrationsserver>. Diese Profile können nicht geändert oder gelöscht werden.

Im Profil <Autonomer-Modus> ist kein Server für die Verbindung angegeben. Daher versucht der Administrationsagent beim Umschalten auf dieses Profil nicht, eine Verbindung zu einem Administrationsserver herzustellen, während auf Client-Geräten installierte Programme unter Mobilen Richtlinien ausgeführt werden. Das Profil <Autonomer-Modus> wird übernommen, wenn die Geräte vom Netzwerk getrennt sind.

Das Profil <Home-Administrationsserver> gibt die Verbindung für den Administrationsserver an, der bei der Installation des Administrationsagenten festgelegt ausgewählt wurde. Das Profil <Home-Administrationsserver> wird verwendet, wenn ein Gerät in einem anderen Netzwerk erneut eine Verbindung zum Home-Administrationsserver herstellt.

5. Passen Sie im folgenden Fenster **Profil konfigurieren** die Einstellungen des Verbindungsprofils an:

- **Profilname**

  In diesem Eingabefeld können Sie sich den Namen des Verbindungsprofils anzeigen lassen oder ihn ändern.

- **Adresse des Administrationsservers**

  Adresse des Administrationsservers, zu dem das Client-Gerät eine Verbindung bei der Aktivierung des Profils herstellen soll.

- **Port**

  Nummer des Ports, über den die Verbindung erfolgt.

- **SSL-Port**

  Nummer des Ports, wenn die Verbindung mit dem SSL-Protokoll erfolgt.

- **SSL-Verbindung verwenden**

  Wenn Sie die Option aktivieren, erfolgt die Verbindung über einen gesicherten Port (mit SSL-Protokoll).

  Diese Option ist standardmäßig aktiviert. Wir empfehlen, diese Option nicht zu deaktivieren, damit Ihre Verbindung gesichert bleibt.

- Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

  - **Adresse**

    Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center mit dem Internet.

  - **Port**

    Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center hergestellt wird.

  - **Authentifizierung am Proxyserver**

    Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  - **Benutzername**

    Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

  - **Kennwort**

    Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

    Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

- **Adresse des Verbindungs-Gateways**

  Gateway-Adresse, über die Client-Geräte mit dem Administrationsserver verbunden werden.

- **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**

  Aktivieren Sie dieses Kontrollkästchen, damit bei der Verbindung von Programmen, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte, die sich im Modus für mobile Benutzer befinden, verwendet werden und die mobile Richtlinie verwendet wird, wenn der Administrationsserver nicht verfügbar ist. Wurde für das Programm keine Richtlinie für mobile Benutzer definiert, verwendet das Programm die aktive Richtlinie.

  Wenn diese Option deaktiviert ist, wenden die Anwendungen die aktiven Richtlinien an.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Nur für Update-Download verwenden**

  Wenn diese Option aktiviert ist, wird das Profil nur beim Update-Download von den auf dem Client-Gerät installierten Programmen verwendet. Bei den übrigen Vorgängen erfolgt eine Verbindung mit dem Administrationsserver mit den ursprünglichen Verbindungseinstellungen, die bei der Installation des Administrationsagenten eingegeben wurden.

  Diese Option ist standardmäßig aktiviert.

- **Verbindungseinstellungen mit den Einstellungen für den Administrationsserver synchronisieren, die in diesem Profil angegeben sind**

  Wenn diese Option aktiviert ist, stellt der Administrationsagent eine Verbindung zum Administrationsserver her und verwendet dazu die Einstellungen, die in den Profileigenschaften angegeben sind.

  Wenn diese Option deaktiviert ist, stellt der Administrationsagent eine Verbindung zum Administrationsserver mithilfe der bei der Installation angegebenen ursprünglichen Einstellungen her.

  Diese Option ist verfügbar, wenn die Option **Nur für Update-Download verwenden** aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

Für mobiler Benutzer wird ein Profil zur Verbindung des Administrationsagenten zum Administrationsserver erstellt. Wird mit diesem Profil eine Verbindung des Administrationsagenten zum Administrationsserver hergestellt, so verwenden die auf dem Client-Gerät installierten Programme Richtlinien für Geräte, die sich im Modus für mobile Benutzer befinden, oder mobile Richtlinien.

Über das Umschalten eines Administrationsagenten auf einen anderen Administrationsserver

In Kaspersky Security Center besteht die Möglichkeit, den Administrationsagenten eines Client-Geräts bei einer Änderung der folgenden Netzwerkeigenschaften auf andere Administrationsserver umzuschalten:

- **Bedingung für die DHCP-Serveradresse** – Änderung der IP-Adresse für den DHCP-Server (Dynamic Host Configuration Protocol) im Netzwerk.
- **Bedingung für die standardmäßige Adresse des Verbindungs-Gateways** – Änderung des Standard-Gateways im Netzwerk.
- **Bedingung für DNS-Domäne** – Änderung des DNS-Suffixes im Subnetz.
- **Bedingung für die DNS-Serveradresse** – Änderung der IP-Adresse für den DNS-Server im Netzwerk.
- **Bedingung für die WINS-Serveradresse** – Änderung der IP-Adresse für den WINS-Server im Netzwerk. Diese Einstellung ist nur auf Windows-Geräten verfügbar.
- **Bedingung für die Namensauflösung** – Änderung des DNS- oder NetBIOS-Namens des Client-Geräts.
- **Bedingung für Subnetz** – Änderung der Adresse und Subnetzmaske.
- **Bedingung für die Erreichbarkeit der Windows-Domäne** – Änderung des Status der Windows-Domäne, mit der das Client-Gerät verbunden ist. Diese Einstellung ist nur auf Windows-Geräten verfügbar.
- **Bedingung für Verfügbarkeit der SSL-Verbindungsadresse** – Das Client-Gerät kann oder kann nicht (in Abhängigkeit der von Ihnen gewählten Option) eine SSL-Verbindung zu einem Server (Name:Port) herstellen. Sie müssen einen dedizierten Server und eine Software verwenden, die hohen Auslastungen und häufigen Verbindungsanfragen des Administrationsagenten gewachsen ist. Geben Sie nicht den Port des Administrationsservers an. Sie können für jeden Server ein zusätzliches SSL-Zertifikat hinzufügen. In diesem Fall verifiziert der Administrationsagent das Serverzertifikat zusätzlich zur Prüfung auf eine mögliche SSL-Verbindung. Wenn das Zertifikat nicht übereinstimmt, schlägt die Verbindung fehl.

Diese Funktion wird nur für Administrationsagenten unterstützt, die auf Geräten unter Windows oder macOS installiert sind.

Bei der Installation des Administrationsagenten werden die ursprünglichen Verbindungseinstellungen des Administrationsagenten mit dem Administrationsserver eingegeben. Sobald die Regeln für die Umstellung des Administrationsagenten mit anderen Administrationsservern definiert wurden, reagiert der Agent auf die Änderungen der Netzwerkeigenschaften folgendermaßen:

- Wenn die Netzwerkeigenschaften einer der erstellten Regeln entsprechen, wird der Administrationsagent mit dem in der Regel vorgegebenen Administrationsserver verbunden. Die auf den Client-Geräten installierten Anwendungen wechseln zu den Richtlinien für mobile Benutzer, wenn dies durch eine Regel vorgegeben wurde.
- Wird keine Regel ausgeführt, wird der Administrationsagent auf die ursprünglichen Verbindungseinstellungen mit dem Administrationsserver zurückgesetzt, die bei der Installation vorgegeben wurden. Die auf den Client-Geräten installierten Programme werden auf die aktiven Richtlinien zurückgesetzt.
- Ist der Administrationsserver nicht verfügbar, verwendet der Administrationsagent die Richtlinien für mobile Benutzer.

Der Administrationsagent verwendet die Richtlinie für mobile Benutzer nur dann, wenn die Option **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist** in den Einstellungen des Administrationsagenten aktiviert ist.

Die Verbindungseinstellungen des Administrationsagenten mit dem Administrationsserver werden im Verbindungsprofil gespeichert. Im Verbindungsprofil können Sie Regeln für den Wechsel der Client-Geräte zu den Richtlinien für mobile Benutzer erstellen sowie das Profil so einrichten, dass es nur zum Download von Updatedateien verwendet wird.

Erstellen der Regel für die Umstellung des Administrationsagenten gemäß dem Netzwerkspeicherort

Die Umstellung des Administrationsagenten gemäß des Netzwerkspeicherorts ist nur auf Geräten verfügbar, die unter Windows und macOS laufen.

Um eine Regel für die Umstellung des Administrationsagenten von einem Administrationsserver auf einen anderen bei geänderten Eigenschaften des Netzwerks anzulegen, gehen Sie wie folgt vor:

1. Wenn Sie eine Regel für eine Gruppe verwalteter Geräte erstellen möchten, öffnen Sie die Richtlinie des Administrationsagenten dieser Gruppe. Gehen Sie dafür folgendermaßen vor:

   a. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

   b. Klicken Sie auf den Link des aktuellen Pfads.

   c. Wählen Sie im sich öffnenden Fenster die erforderliche Administrationsgruppe aus.

   Anschließend wird der aktuelle Pfad geändert.

   d. Fügen Sie die Richtlinie des Administrationsagenten für die Gruppe der verwalteten Geräte hinzu. Wenn Sie diese bereits erstellt haben, klicken Sie auf den Namen der Richtlinie des Administrationsagenten, um ihre Eigenschaften zu öffnen.

2. Wenn Sie eine Regel für ein bestimmtes verwaltetes Gerät erstellen möchten, gehen Sie wie folgt vor:

   a. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   b. Klicken Sie auf den Namen des verwalteten Geräts.

   c. Wechseln Sie im sich öffnenden Eigenschaftenfenster des verwalteten Geräts auf die Registerkarte **Programme**.

   d. Klicken Sie auf den Namen der Richtlinie des Administrationsagenten, für die nur das ausgewählte verwaltete Gerät gilt.

3. Wechseln Sie im sich öffnenden Eigenschaftenfenster zu **Programmeinstellungen** → **Konnektivität** → **Verbindungsprofile.**

4. Klicken Sie im Abschnitt **Einstellungen des Netzwerkstandorts** auf **Hinzufügen**.

5. Passen Sie im folgenden Eigenschaftenfenster die Einstellungen der Beschreibungen des Netzwerkspeicherorts und der Regel der Umschaltung an. Passen Sie die folgenden Einstellungen der Beschreibungen des Netzwerkspeicherorts an:

   - **Beschreibung**

     Der Name der Beschreibungen des Netzwerkspeicherorts darf nicht mehr als 255 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\/:|).

   - **Folgendes Verbindungsprofil verwenden**

     In dieser Dropdown-Liste können Sie ein Verbindungsprofil des Administrationsagenten mit dem Administrationsserver auswählen. Das Profil wird beim Ausführen der Bedingungen der Beschreibungen des Netzwerkspeicherorts verwendet. Das Verbindungsprofil umfasst die Verbindungen des Administrationsagenten für den Administrationsserver und bestimmt den Wechsel der Client-Geräte auf mobile Richtlinien. Das Profil wird nur zum Download von Updates verwendet.

   - **Beschreibung aktiv**

     Aktivieren Sie dieses Kontrollkästchen, um die Verwendung der neuen Beschreibung des Netzwerkstandorts zu aktivieren.

6. Wählen Sie die Bedingungen für die Umschaltregel des Administrationsagenten aus:

   - **Bedingung für die DHCP-Serveradresse** – Änderung der IP-Adresse für den DHCP-Server (Dynamic Host Configuration Protocol) im Netzwerk.

   - **Bedingung für die standardmäßige Adresse des Verbindungs-Gateways** – Änderung des Standard-Gateways im Netzwerk.

   - **Bedingung für DNS-Domäne** – Änderung des DNS-Suffixes im Subnetz.

   - **Bedingung für die DNS-Serveradresse** – Änderung der IP-Adresse für den DNS-Server im Netzwerk.

   - **Bedingung für die WINS-Serveradresse** – Änderung der IP-Adresse für den WINS-Server im Netzwerk. Diese Einstellung ist nur auf Windows-Geräten verfügbar.

   - **Bedingung für die Namensauflösung** – Änderung des DNS- oder NetBIOS-Namens des Client-Geräts.

   - **Bedingung für Subnetz** – Änderung der Adresse und Subnetzmaske.

- **Bedingung für die Erreichbarkeit der Windows-Domäne** – Änderung des Status der Windows-Domäne, mit der das Client-Gerät verbunden ist. Diese Einstellung ist nur auf Windows-Geräten verfügbar.

- **Bedingung für Verfügbarkeit der SSL-Verbindungsadresse** – Das Client-Gerät kann oder kann nicht (in Abhängigkeit der von Ihnen gewählten Option) eine SSL-Verbindung zu einem Server (Name:Port) herstellen. Sie können für jeden Server ein zusätzliches SSL-Zertifikat hinzufügen. In diesem Fall verifiziert der Administrationsagent das Serverzertifikat zusätzlich zur Prüfung auf eine mögliche SSL-Verbindung. Wenn das Zertifikat nicht übereinstimmt, schlägt die Verbindung fehl.

Die Bedingungen in der Regel beruhen auf dem logischen UND-Operator. Damit die Regel zur Umschaltung gemäß der Beschreibung des Netzwerkspeicherorts ausgelöst wird, müssen alle Umschaltbedingungen der Regel erfüllt sein.

7. Geben Sie im Abschnitt mit den Bedingungen an, wann der Administrationsagent auf einen anderen Administrationsserver umgestellt werden soll. Klicken Sie dazu auf die Schaltfläche **Hinzufügen** und legen Sie anschließend den Wert der Bedingung fest.

   Zusätzlich ist die Option **Trifft auf mindestens einen Wert der Liste zu** standardmäßig aktiviert. Sie können diese Option deaktivieren, wenn Sie möchten, dass die Bedingung mit allen angegebenen Werten erfüllt wird.

8. Speichern Sie Ihre Änderungen.

Daraufhin wird eine Regel zur Umschaltung gemäß der Beschreibung des Netzwerkspeicherorts erstellt, und der Administrationsagent verwendet bei Erfüllung der Bedingungen das in der Beschreibung angegebene Verbindungsprofil für die Verbindung mit dem Administrationsserver.

Assistent für die Bereitstellung des Schutzes

Um Kaspersky-Anwendungen zu installieren, können Sie den Assistenten für die Bereitstellung des Schutzes verwenden. Der Assistent für die Bereitstellung des Schutzes ermöglicht die Remote-Installation von Anwendungen entweder mit zuvor speziell erstellten Installationspaketen oder direkt aus den Programmpaketen.

Der Assistent für die Bereitstellung des Schutzes führt die folgenden Aktionen aus:

- Herunterladen eines Installationspaket für die Anwendung (falls es zuvor nicht erstellt wurde). Das Installationspaket befindet sich unter **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**. Dieses Installationspaket kann zur weiteren Installation der Anwendung herangezogen werden.

- Erstellen und starten eine Aufgabe zur Remote-Installation für eine Reihe von Geräten oder für eine Administrationsgruppe. Die soeben erstellte Aufgabe zur Remote-Installation wird in dem Abschnitt **Aufgaben** gespeichert. Sie können diese Aufgabe später manuell starten. Der Aufgabentyp ist **Remote-Installation eines Programms**.

Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

Schritt 1. Assistent für die Bereitstellung des Schutzes starten

So starten Sie den Assistenten für die Bereitstellung des Schutzes manuell:

Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Assistent für die Bereitstellung des Schutzes**.

Der Assistent für die Bereitstellung des Schutzes wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

Schritt 2. Installationspaket auswählen

Wählen Sie das Installationspaket der Anwendung, das Sie installieren möchten.

Wenn das Installationspaket der gewünschten Anwendung nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie anschließend die Anwendung aus der Liste aus.

Schritt 3. Verteilungsmethode der Schlüsseldatei oder des Aktivierungscodes auswählen

Wählen Sie eine Methode zur Verteilung einer Schlüsseldatei oder eines Aktivierungscodes aus:

- **Lizenzschlüssel nicht zum Installationspaket hinzufügen**

  Der Schlüssel wird automatisch auf alle Geräte verteilt, mit denen er kompatibel ist:
  - Wenn in den Eigenschaften des Schlüssel die automatische Verteilung aktiviert ist.
  - Wenn die Aufgabe **Schlüssel hinzufügen** erstellt wurde.

- **Lizenzschlüssel zum Installationspaket hinzufügen**

  Der Schlüssel wird gemeinsam mit dem Installationspaket an Geräte verteilt.

  > Es wird nicht empfohlen, den Schlüssel auf diese Art zu verteilen, da die Datenverwaltung der Installationspakete über allgemeinen Lesezugriff verfügt.

Wenn eine Schlüsseldatei oder ein Aktivierungscode bereits zum Installationspaket gehören, wird dieses Fenster angezeigt; enthält dann aber nur Informationen über den Lizenzschlüssel.

Schritt 4. Auswählen der Version des Administrationsagenten

Wenn Sie das Installationspaket einer anderen Anwendung ausgewählt haben (nicht den Administrationsagenten), müssen Sie auch den Administrationsagenten installieren, da dieser die Anwendung mit dem Kaspersky Security Center Administrationsserver verbindet.

Wählen Sie die aktuellste Version des Administrationsagenten aus.

Schritt 5. Auswählen der Geräte

Geben Sie eine Liste mit Geräte an, auf denen die Anwendung installiert werden soll:

- **Auf verwalteten Geräten installieren**

  Bei Auswahl dieser Option wird die Aufgabe zur Remote-Installation eines Programms für eine Gerätegruppe erstellt.

- **Geräte für die Installation auswählen**

  Die Aufgabe wird Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Schritt 6. Festlegen der Einstellungen für die Aufgabe zur Remote-Installation

Passen Sie auf der Seite **Einstellungen für die Aufgabe zur Remote-Installation** die Einstellungen für die Remote-Installation einer Anwendung.

Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Anwendungsinstallation erforderlichen Dateien auf die Client-Geräte aus:

- **Unter Nutzung des Administrationsagenten**

  Wenn die Option aktiviert ist, werden die Installationspakete von dem auf den Client-Geräten installierten Administrationsagenten zugestellt.

  Wenn diese Option deaktiviert ist, werden Installationspakete mithilfe der Betriebssystems-Tools der Client-Geräte ausgeliefert.

  Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

  Diese Option ist standardmäßig aktiviert.

- **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**

  Wenn diese Option aktiviert ist, werden Installationspakete mithilfe der Tools von den Betriebssystemen durch Verteilungspunkte auf die Geräte übertragen. Diese Variante ist wählbar, wenn sich im Netzwerk mindestens ein Verteilungspunkt befindet.

  Ist die Option **Mithilfe des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Betriebssystem-Tools zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

  Standardmäßig ist diese Option für die Aufgaben von Remote-Installationen aktiviert, die auf einem virtuellen Administrationsserver erstellt wurden.

  > Wenn alle Verteilungspunkte, die einem Gerät zugewiesen wurden, fehlerhaft sind, erhält das Gerät keine Updates (Antiviren-Datenbanken und Patches) und keine Installationspakete.

- **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**

  Wenn diese Option aktiviert ist, werden die Dateien durch den Administrationsserver mittels Betriebssystem-Tools der Client-Gerät auf die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

  Diese Option ist standardmäßig aktiviert.

Passen Sie die erweiterten Einstellungen an:

- **Programm nicht neu installieren, wenn es bereits installiert ist**

  Wenn diese Option aktiviert ist, wird die ausgewählte Anwendung nicht neu installiert, wenn sie bereits auf dem Client-Gerät installiert ist.

  Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Anwendung in jedem Fall installiert.

  Diese Option ist standardmäßig aktiviert.

- **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen**

  Wenn diese Option aktiviert ist, wird das Installationspaket mithilfe von Richtlinien des Active Directory installiert.

  Die Option ist verfügbar, wenn ein Installationspaket des Administrationsagenten ausgewählt ist.

  Diese Option ist standardmäßig deaktiviert.

Schritt 7. Verwaltung des Neustarts

Geben Sie an, welche Aktion ausgeführt werden soll, wenn das Betriebssystem bei der Installation des Programms neu gestartet werden muss:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen nach (Min.)**

    Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

    Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neu starten nach (Min.)**

    Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

    Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

Schritt 8. Deinstallieren inkompatibler Programme vor der Installation

Dieser Schritt ist nur dann verfügbar, wenn das zu verteilende Programm bekanntlich mit anderen Programmen inkompatibel ist.

Wählen Sie diese Option, wenn Sie möchten, dass Kaspersky Security Center automatisch Programme deinstalliert, die mit dem zu verteilenden Programm inkompatibel sind.

Die Liste der inkompatiblen Programme wird ebenfalls angezeigt.

Wenn Sie diese Option nicht auswählen, wird das Programm nur auf Geräten installiert, die keine inkompatiblen Programme aufweisen.

Schritt 9. Verschieben von Geräten in die Gruppe "Verwaltete Geräte"

Geben Sie an, ob die Geräte nach Abschluss der Installation des Administrationsagenten in die Administrationsgruppe verschoben werden müssen.

- **Geräte nicht verschieben**

  Die Geräte bleiben in den Gruppen, in denen sie sich gerade befinden. Die Geräte, die keiner Gruppe zugeordnet wurden, bleiben nicht zugeordnet.

- **Nicht zugeordnete Geräte in eine Gruppe verschieben**

  Die Geräte werden in die ausgewählte Administrationsgruppe verschoben.

Die Variante **Geräte nicht verschieben** ist standardmäßig festgelegt. Aus Sicherheitsgründen sollten Sie die Geräte manuell verschieben.

Schritt 10. Auswählen von Benutzerkonten für den Zugriff auf Geräten

Bei Bedarf können Sie Benutzerkonten hinzufügen, die für den Start der Aufgabe zur Remote-Installation verwendet werden sollen:

- **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

  Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm der Anwendung gestartet werden soll. Die Aufgabe wird unter dem Konto gestartet, unter dem der Dienst des Administrationsservers läuft.

  Wenn der Administrationsagent nicht auf den Client-Geräten installiert ist, steht diese Option nicht zur Verfügung.

- **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**

  Wählen Sie diese Option, wenn auf den Geräten, denen Sie die Aufgabe zur Remote-Installation zuweisen, der Administrationsagent nicht installiert ist. In diesem Fall können Sie ein Benutzerkonto oder ein SSH-Zertifikat angeben, um die Anwendung zu installieren.

  - **Lokales Benutzerkonto**. Wenn Sie diese Variante auswählen, können Sie das Benutzerkonto angeben, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Benutzerkonto** aus, und geben Sie anschließend die Anmeldeinformationen des Benutzerkontos an.

    Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Benutzerkonto existiert, dass über die erforderlichen Rechte auf allen Geräten verfügt, für welche die Aufgabe bestimmt wurde. In diesem Fall werden für den Start der Aufgabe alle hinzugefügten Konten nacheinander von oben nach unten angewandt.

- **SSH-Zertifikat**. Wenn Sie eine Anwendung auf einem Linux-basierten Client-Gerät installieren möchten, können Sie anstelle eines Benutzerkontos ein SSH-Zertifikat angeben. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **SSH-Zertifikat** aus, und geben Sie anschließend den privaten und den öffentlichen Schlüssel des Zertifikats an.

  Um einen privaten Schlüssel zu generieren, können Sie das Tool "ssh-keygen" verwenden. Beachten Sie, dass die Kaspersky Security Center das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" den Parameter "-m PEM" hinzu. Beispielsweise:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< Benutzer-E-Mail >"
  ```

Schritt 11. Installation starten

Dies ist der abschließende Schritt des Assistenten. In diesem Schritt wurde die **Aufgabe zur Remote-Installation** erfolgreich erstellt und konfiguriert.

Die Variante **Aufgabe nach Abschluss des Assistenten starten** ist standardmäßig nicht ausgewählt. Wenn Sie diese Option auswählen, startet die **Aufgabe zur Remote-Installation** sofort nach Abschluss des Assistenten. Wenn Sie diese Option nicht auswählen, startet die **Aufgabe zur Remote-Installation** nicht. Sie können diese Aufgabe später manuell starten.

Klicken Sie auf **OK**, um den letzten Schritt des Assistenten für die Bereitstellung des Schutzes abzuschließen.

Bereitstellung der Kaspersky-Anwendungen über die Kaspersky Security Center Web Console

Dieser Abschnitt beschreibt die Bereitstellung von Kaspersky-Anwendungen auf Client-Geräten in Ihrem Unternehmen mithilfe von Kaspersky Security Center Web Console.

Szenario: Softwareverteilung der Programme von Kaspersky über die Kaspersky Security Center Web Console

Dieses Szenario erklärt, wie Kaspersky-Anwendungen über Kaspersky Security Center Web Console verteilt werden. Sie können den Schnellstartassistenten und den Assistenten für die Bereitstellung des Schutzes verwenden oder alle erforderlichen Schritte manuell ausführen.

Die folgenden Programme können über die Kaspersky Security Center Web Console verteilt werden:

- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security für Linux

Schritte

Die Bereitstellung von Kaspersky-Anwendungen erfolgt schrittweise:

1. **Download des Verwaltungs-Plug-ins für das Programm**

   Diese Etappe ist Teil des Schnellstartassistenten. Wenn Sie den Assistenten nicht ausführen möchten, laden Sie das Plug-in für Kaspersky Endpoint Security für Windows manuell herunter.

   Wenn Sie mobile Unternehmensgeräte verwalten möchten, folgen Sie den Anweisungen in der Hilfe von Kaspersky Security für mobile Endgeräte, um die Verwaltungs-Plug-ins von Kaspersky Endpoint Security für Android herunterzuladen und zu installieren.

2. **Installationspakete herunterladen und erstellen**

   Diese Etappe ist Teil des Schnellstartassistenten.

   Mithilfe des Schnellstartassistenten können Sie das Installationspaket mit dem Verwaltungs-Plug-in herunterladen. Wenn Sie diese Option beim Ausführen des Assistenten nicht ausgewählt haben oder wenn Sie den Assistenten nicht ausgeführt haben, müssen Sie das Paket manuell herunterladen.

   Wenn die Installation von Kaspersky-Anwendungen mithilfe von Kaspersky Security Center auf bestimmten Geräten nicht möglich ist (z. B. auf Geräten von Remote-Mitarbeitern), können Sie autonome Installationspakete für Anwendungen erstellen. Wenn Sie für die Installation von Kaspersky-Anwendungen autonome Pakete verwenden, müssen Sie weder eine Aufgabe zur Remote-Installation erstellen und ausführen noch Aufgaben für Kaspersky Endpoint Security für Windows erstellen und konfigurieren.

3. **Erstellen, Konfigurieren und Ausführen der Remote-Installationsaufgabe**

   In Kaspersky Endpoint Security für Windows ist dieser Schritt Teil des Assistenten für die Bereitstellung des Schutzes, der automatisch gestartet wird, nachdem der Schnellstartassistent abgeschlossen wurde. Wenn Sie den Assistenten für die Bereitstellung des Schutzes nicht ausführen möchten, müssen Sie diese Aufgabe manuell erstellen und konfigurieren.

   Manuell können Sie mehrere Remote-Installationsaufgaben für verschiedene Administrationsgruppen oder unterschiedliche Geräteauswahlen erstellen. Sie können in diesen Aufgaben verschiedene Versionen einer Anwendung bereitstellen.

   Stellen Sie sicher, dass alle Geräte in Ihrem Netzwerk erkannt wurden. Starten Sie dann die Aufgabe (Aufgaben) zur Remote-Installation.

   > Installieren Sie auf Ihren Linux-basierten Assets das Tool "nmap". Dieses Tool ist erforderlich, um die NLA-Funktion (Network Location Awareness) zu aktivieren.

   > Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

   > Wenn Sie den Administrationsagenten auf Geräten mit den Betriebssystemen RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher installieren möchten, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsagent ordnungsgemäß funktioniert.

4. **Erstellen und konfigurieren der Aufgaben für das verwaltete Programm**

   Die Aufgabe *Update installieren* von Kaspersky Endpoint Security für Windows muss konfiguriert werden.

Dieser Schritt ist Teil des Schnellstartassistenten: Die Aufgabe wird automatisch mit den Standardeinstellungen erstellt und konfiguriert. Wenn Sie den Assistenten nicht ausgeführt haben, müssen Sie diese Aufgabe manuell erstellen und auch manuell konfigurieren. Wenn Sie den Schnellstartassistenten verwenden, stellen Sie sicher, dass der Zeitplan für die Aufgabe Ihren Anforderungen entspricht (Standardmäßig ist der geplante Start für die Aufgabe auf **Manuell** eingestellt; möglicherweise möchten Sie eine andere Option auswählen).

Andere Kaspersky-Anwendungen haben möglicherweise andere Standardaufgaben. Einzelheiten entnehmen Sie bitte der Dokumentation zu den entsprechenden Anwendungen.

Stellen Sie sicher, dass der Zeitplan für jede erstellte Aufgabe Ihren Anforderungen entspricht.

5. **Installieren von Kaspersky Security für mobile Endgeräte (optional)**

   Wenn Sie mobile Unternehmensgeräte verwalten möchten, folgen Sie den Anweisungen in der Hilfe von Kaspersky Security für mobile Endgeräte, um Informationen zur Bereitstellung von Kaspersky Endpoint Security für Android zu erhalten.

6. **Richtlinien anlegen**

   Erstellen Sie die Richtlinie für jedes Programm manuell oder (für Kaspersky Endpoint Security für Windows) über den Schnellstartassistenten. Sie können die Standardeinstellungen der Richtlinie verwenden. Sie können jedoch die Standardeinstellungen der Richtlinie jederzeit gemäß Ihren Anforderungen ändern.

7. **Untersuchung der Ergebnisse**

   Stellen Sie sicher, dass die Bereitstellung erfolgreich beendet wurde: Jedes Programm besitzt Richtlinien und Aufgaben und diese Programme sind auf den verwalteten Geräten installiert.

Ergebnisse

Der Abschluss des Szenarios bringt folgende Ergebnisse mit sich:

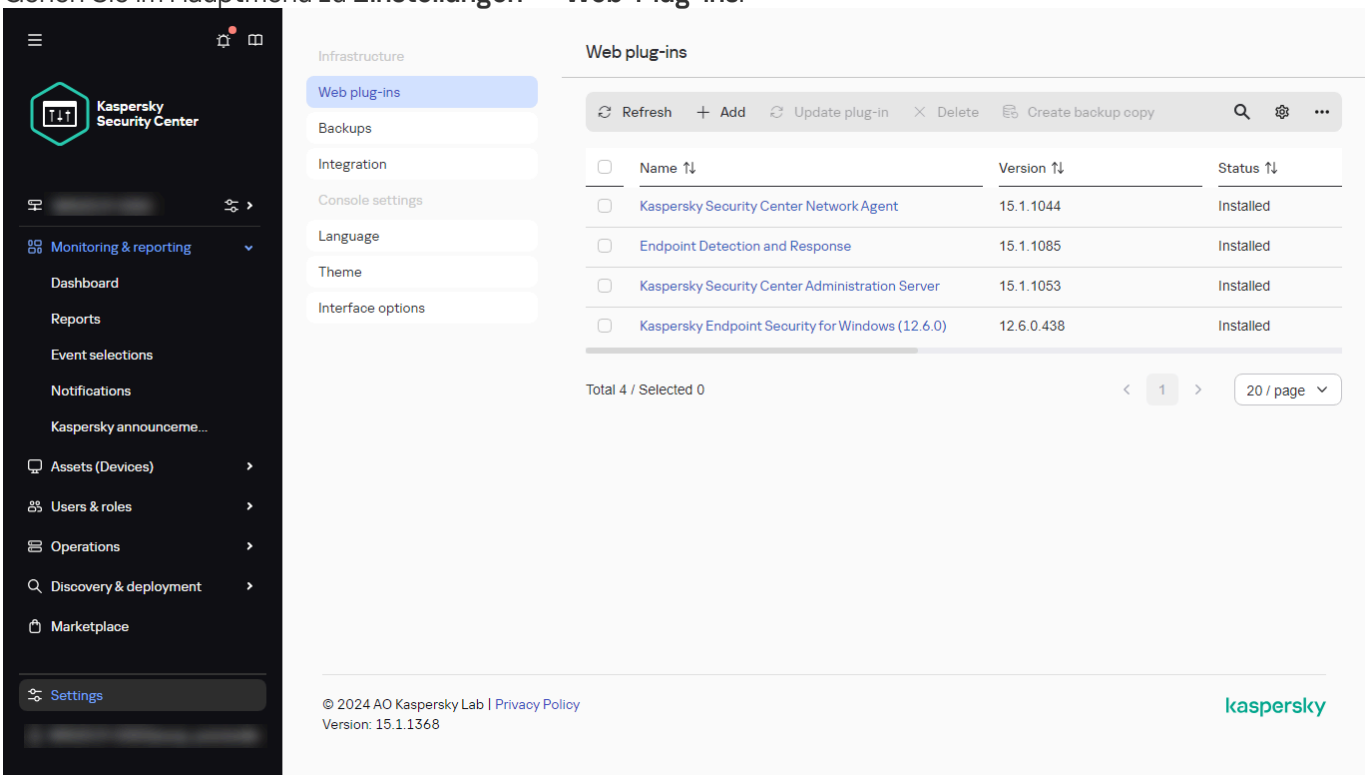
- Es werden alle erforderlichen Richtlinien und Aufgaben für die ausgewählten Anwendungen erstellt.
- Die Zeitpläne der Aufgaben werden gemäß Ihren Anforderungen angepasst.
- Die ausgewählten Programme wurden auf den ausgewählten Client-Geräten verteilt oder werden nach Zeitplan verteilt.

Beziehen von Plug-ins für Kaspersky-Anwendungen

Um eine Kaspersky-Anwendung wie Kaspersky Endpoint Security für Windows zu installieren, müssen Sie das Verwaltungs-Plug-in für diese Anwendung herunterladen.

So laden Sie ein Verwaltungs-Plug-in für eine Kaspersky-Anwendung herunter:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Web-Plug-ins**.



Die Liste der installierten Web-Plug-ins

2. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

   Eine Liste der verfügbaren Plug-ins wird angezeigt.

3. Wählen Sie in der Liste der verfügbaren Plug-ins das Plug-in aus, das Sie herunterladen möchten (z. B. Kaspersky Endpoint Security 11 für Windows), indem Sie auf seinen Namen klicken.

   Die Seite mit der Beschreibung des Plug-ins wird angezeigt.

4. Klicken Sie auf der Seite mit der Beschreibung des Plug-ins auf **Plug-in installieren**.

5. Klicken Sie nach Abschluss der Installation auf **OK**.

Das Verwaltungs-Plug-in wird mit der Standardkonfiguration heruntergeladen und in der Liste mit Verwaltungs-Plug-ins angezeigt.

Sie können Plug-ins hinzufügen und heruntergeladene Plug-ins aus einer Datei aktualisieren. Verwaltungs-Plug-ins, bzw. die Web-Versionen von Verwaltungs-Plug-ins können Sie von der Webseite des Technischen Supports von Kaspersky herunterladen.

So können Sie Plug-ins herunterladen oder aus einer Datei aktualisieren:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Web-Plug-ins**.

2. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf **Aus Datei hinzufügen**, um ein Plug-in aus einer Datei herunterzuladen.
   - Klicken Sie auf **Aus Datei aktualisieren**, um das Update für ein Plug-in aus einer Datei herunterzuladen.

3. Geben Sie die Datei und die Dateisignatur an.

4. Laden Sie die angegebenen Dateien herunter.

Das Verwaltungs-Plug-in wird aus der Datei heruntergeladen und in der Liste mit Verwaltungs-Plug-ins angezeigt.

Installationspakete für Kaspersky-Anwendungen herunterladen und erstellen

Wenn Ihr Administrationsserver über einen Internetzugang verfügt, können Sie die Installationspakete für Kaspersky-Anwendungen über die Kaspersky-Webserver erstellen.

Um ein Installationspaket für eine Kaspersky-Anwendung herunterzuladen und zu erstellen:

1. Führen Sie eine der folgenden Aktionen aus:

   - Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.

   - Gehen Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Installationspakete**.

   Benachrichtigungen über neue Pakete für Kaspersky-Anwendungen können Sie auch in der Liste der Benachrichtigungen auf dem Bildschirm anzeigen. Wenn es Benachrichtigungen über ein neues Paket gibt, können Sie auf den Link neben der Benachrichtigung klicken und zur Liste der verfügbaren Installationspakete wechseln.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen eines Installationspakets wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie die Option **Installationspaket für ein Programm von Kaspersky erstellen**.

   Eine Liste der Installationspakete, die auf den Kaspersky-Webservern verfügbar sind, wird angezeigt. Die Liste enthält nur Installationspakete von den Programmen, die zu der aktuell genutzten Version von Kaspersky Security Center kompatibel sind.

4. Klicken Sie auf den Namen eines Installationspakets, z. B. Kaspersky Endpoint Security für Windows (11.1.0).

   Ein Fenster mit Informationen über das Installationspaket wird geöffnet.

   > Sie können ein Installationspaket mit kryptografischen Tools, die eine starke Verschlüsselung implementieren, herunterladen und verwenden, wenn es den geltenden Gesetzen und Vorschriften entspricht. Um ein Installationspaket von Kaspersky Endpoint Security für Windows herunterzuladen, dass den Bedürfnissen Ihrer Organisation entspricht, konsultieren Sie die Gesetzgebung in dem Land, in dem sich die Client-Geräte Ihrer Organisation befinden.

5. Lesen Sie die Informationen und klicken Sie auf **Herunterladen und Installationspaket erstellen**.

   Wenn ein Programmpaket nicht in ein Installationspaket konvertiert werden kann, wird die Schaltfläche **Programmpaket herunterladen** anstelle der Schaltfläche **Herunterladen und Installationspaket erstellen** angezeigt.

Der Download des Installationspakets auf den Administrationsserver beginnt. Sie können das Fenster des Assistenten schließen, oder mit dem nächsten Schritt der Anleitung fortfahren. Wenn sie das Fenster des Assistenten schließen, wird der Download im Hintergrund fortgesetzt.

Um den Fortschritt des Downloadvorgangs des Installationspakets zu verfolgen:

a. Gehen Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Installationspakete** → **In Bearbeitung ()**.

b. Sie können den Fortschritt in den Spalten **Download-Fortschritt** und **Download-Status** der Tabelle verfolgen.

Wenn der Vorgang abgeschlossen ist, wird das Installationspaket der Liste auf der Registerkarte **Heruntergeladen** hinzugefügt. Wenn der Downloadvorgang anhält und der Downloadstatus zu **EULA akzeptieren** wechselt, klicken Sie auf den Namen des Installationspakets und fahren Sie mit dem nächsten Schritt der Anleitung fort.

Wenn die Datenmenge im ausgewählten Programmpaket die aktuelle Begrenzung übersteigt, wird eine Fehlermeldung angezeigt. Sie können den Wert der Begrenzung ändern und anschließend mit der Erstellung des Installationspaketes fortfahren.

6. Bei einigen Kaspersky-Anwendungen wird während des Downloads die Schaltfläche **EULA anzeigen** angezeigt. Wird diese angezeigt, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **EULA anzeigen**, um den Endbenutzer-Lizenzvertrag (EULA) zu lesen.

   b. Lesen Sie die EULA, die auf dem Bildschirm angezeigt wird, und klicken Sie auf **Akzeptieren**.

      Der Download wird fortgesetzt, nachdem Sie die EULA akzeptiert haben. Wenn Sie auf **Ablehnen** klicken, wird der Download beendet.

7. Wenn der Download abgeschlossen ist, klicken Sie auf die Schaltfläche **Schließen**.

Das ausgewählte Installationspaket wird in den freigegebenen Ordner des Administrationsservers in den Unterordner "Packages" heruntergeladen. Nach dem Download wird das Installationspaket in der Liste der Installationspakete angezeigt.

Größenbegrenzung für benutzerdefinierte Installationspakete anpassen

Die Gesamtgröße der während der Erstellung eines benutzerdefinierten Installationspakets entpackten Daten ist begrenzt. Das Standardlimit beträgt 1 GB.

Wenn Sie versuchen ein Archiv hochzuladen, dessen beinhalteten Daten die aktuelle Begrenzung übersteigen, wird eine Fehlermeldung angezeigt. Wenn Sie Installationspakete aus großen Programmpaketen erstellen, müssen Sie unter Umständen den Grenzwert erhöhen.

Um den Grenzwert für benutzerdefinierte Installationspakete zu ändern:

1. Führen Sie auf dem Gerät des Administrationsservers die Eingabeaufforderung unter dem Konto aus, dass verwendet wurde, um den Administrationsserver zu installieren.

2. Ändern Sie Ihr aktuelles Verzeichnis in den Installationsordner von Kaspersky Security Center (standardmäßig <Laufwerk>:\Programme (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Geben Sie je nach Art der Installation des Administrationsservers einen der folgenden Befehle mit Administratorrechten ein:

   - Gewöhnliche lokale Installation:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <Anzahl an Bytes>
     ```

   - Auf einem Kaspersky Security Center Failover-Cluster installieren:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <Anzahl an Bytes> --stp klfoc
     ```

   - Auf einem Windows Server Failover-Cluster installieren:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <Anzahl an Bytes> --stp cluster
     ```

   Wobei <Anzahl an Bytes> eine Anzahl an Bytes im Hexadezimal- oder Dezimalformat ist.

   Wenn das erforderliche Limit beispielsweise 2 GB beträgt, können Sie den Dezimalwert 2147483648 oder den Hexadezimalwert 0x80000000 angeben. In diesem Fall können Sie für eine lokale Installation des Administrationsservers den folgenden Befehl verwenden:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Die Größenbegrenzung für benutzerdefinierte Installationspakete wird geändert.

Programmpakete für Kaspersky-Anwendungen herunterladen

In der Kaspersky Security Center Web Console können Sie Programmpakete für Kaspersky-Anwendungen herunterladen und speichern. Sie können die Programme mithilfe der Programmpakete auch manuell installieren, ohne Kaspersky Security Center zu verwenden.

Um Programmpakete für Kaspersky-Anwendungen herunterzuladen und zu speichern, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Kaspersky-Anwendungen** → **Aktuelle Anwendungsversionen**.

   Eine Liste mit verfügbaren Programmpaketen, Plug-ins und Patches wird geöffnet. Kaspersky Security Center zeigt nur die Objekte an, die mit seiner aktuell verwendeten Version kompatibel sind.

2. Klicken Sie in der Liste auf den Namen des Pakets, das Sie herunterladen möchten.

   Die Beschreibung des Pakets wird geöffnet.

3. Lesen Sie die Beschreibung und klicken Sie auf **Herunterladen und Installationspaket erstellen**.

   Wenn ein Programmpaket nicht in ein Installationspaket konvertiert werden kann, wird die Schaltfläche **Programmpaket herunterladen** anstelle **Herunterladen und Installationspaket erstellen** angezeigt.

   Der Download des Installationspakets auf den Administrationsserver beginnt.

Das ausgewählte Installations- oder Programmpaket wird in den freigegebenen Ordner des Administrationsservers in den Unterordner "**Packages**" heruntergeladen. Nach Abschluss des Downloads wird das Installationspaket in der Liste der Installationspakete angezeigt.

Die erfolgreiche Bereitstellung von Kaspersky Endpoint Security überprüfen

Um sicherzustellen, dass die Kaspersky-Anwendungen (z. B. Kaspersky Endpoint Security) ordnungsgemäß verteilt wurden, gehen Sie wie folgt vor:

1. Vergewissern Sie sich mit der Kaspersky Security Center Web Console, dass Sie über Folgendes verfügen:
   - Eine Richtlinie für Kaspersky Endpoint Security und/oder andere Sicherheitsanwendungen, die Sie nutzen.
   - Aufgaben für Kaspersky Endpoint Security für Windows: *Schnelle Untersuchung* und *Update installieren* (falls Sie Kaspersky Endpoint Security für Windows nutzen).
   - Aufgaben für andere Sicherheitsanwendungen, die Sie nutzen.
2. Stellen Sie auf einem der verwalteten Geräte, das für die Installation ausgewählt wurde, Folgendes sicher:
   - Kaspersky Endpoint Security oder eine andere Sicherheitsanwendung von Kaspersky wurde installiert.
   - Die Einstellungen in Kaspersky Endpoint Security für den Schutz vor bedrohlichen Dateien, für den Schutz vor Web-Bedrohungen und für den Schutz vor E-Mail-Bedrohungen stimmen mit der Richtlinie überein, die Sie für dieses Gerät erstellt haben.
   - Der Kaspersky Endpoint Security-Dienst kann manuell gestoppt und gestartet werden.
   - Gruppenaufgaben können manuell gestoppt und gestartet werden.

Autonome Installationspakete erstellen

Sie und die Gerätebenutzer in Ihrem Unternehmen können autonome Installationspakete verwenden, um Anwendungen manuell auf Geräten zu installieren.

Ein autonomes Installationspaket ist eine ausführbare Datei (installer.exe). Sie können diese Datei auf dem Webserver oder in einem freigegebenen Ordner speichern, per E-Mail verschicken oder auf andere Weise an ein Client-Gerät übertragen. Auf dem Client-Gerät kann der Benutzer die empfangene Datei lokal ausführen, um ohne Beteiligung von Kaspersky Security Center eine Anwendung zu installieren. Sie können jetzt autonome Installationspakete für Kaspersky-Anwendungen und von Drittanbietern für Windows-, macOS- und Linux-Plattformen erstellen. Um ein autonomes Installationspaket für ein Drittanbieter-Programm zu erstellen, müssen Sie ein benutzerdefiniertes Installationspaket erstellen.

Stellen Sie sicher, dass unbefugte Personen keinen Zugriff auf das autonome Installationspaket haben.

So erstellen Sie ein autonomes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Wählen Sie in der Liste der Installationspakete ein Installationspaket aus und klicken Sie oberhalb der Liste auf **Bereitstellen**.

3. Wählen Sie die Option **Unter Nutzung eines autonomen Pakets** aus.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

4. Stellen Sie sicher, dass die Option **Administrationsagent gemeinsam mit diesem Programm installieren** aktiviert ist, wenn Sie den Administrationsagenten zusammen mit der ausgewählten Anwendung installieren möchten.

   > Die Option wird abhängig von der Anwendung angezeigt, für die Sie ein autonomes Installationspaket erstellen.

   Diese Option ist standardmäßig aktiviert. Wir empfehlen, diese Option zu aktivieren, wenn Sie nicht sicher sind, ob der Administrationsagent auf dem Gerät installiert ist. Falls der Administrationsagent bereits auf dem Gerät installiert ist, wird der Administrationsagent auf die neue Version aktualisiert, nachdem das autonome Installationspaket mit dem Administrationsagenten installiert wurde.

   Wenn Sie diese Option deaktivieren, wird der Administrationsagent nicht auf dem Gerät installiert und das Gerät wird nicht verwaltet.

   Falls auf dem Administrationsserver bereits ein autonomes Installationspaket für die ausgewählte Anwendung vorhanden ist, werden Sie vom Assistenten darüber informiert. In diesem Fall müssen Sie eine der folgenden Aktionen auswählen:

   - **Autonomes Installationspaket erstellen**. Wählen Sie diese Option beispielsweise dann aus, wenn Sie ein autonomes Installationspaket für eine neue Anwendungsversion erstellen und dabei ein autonomes Installationspaket beibehalten möchten, das Sie für eine ältere Anwendungsversion erstellt haben. Das neue autonome Installationspaket wird in einem anderen Ordner abgelegt.
   - **Vorhandenes autonomes Installationspaket verwenden**. Wählen Sie diese Option aus, wenn Sie ein vorhandenes autonomes Installationspaket verwenden möchten. Der Vorgang zur Paket-Erstellung wird nicht gestartet.
   - **Vorhandenes autonomes Installationspaket erneut erstellen**. Wählen Sie diese Option aus, wenn Sie ein autonomes Installationspaket für dieselbe Anwendung erneut erstellen möchten. Das autonome Installationspaket wird im selben Ordner abgelegt.

5. Standardmäßig ist im Schritt **In die Liste mit verwalteten Geräten verschieben** die Option **Geräte nicht verschieben** aktiviert. Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten nicht in Administrationsgruppen verschieben möchten, lassen Sie diese Option aktiviert.

   Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten verschieben möchten, wählen Sie die Option **Nicht zugeordnete Geräte in folgende Gruppe verschieben** aus und geben Sie die Administrationsgruppe an, in die Sie das Client-Gerät nach der Installation des Administrationsagenten verschieben möchten. Standardmäßig wird das Gerät in die Gruppe **Verwaltete Geräte** verschoben.

6. Wenn die Erstellung des autonomen Installationspakets abgeschlossen ist, klicken Sie auf die Schaltfläche **ABSCHLIESSEN**.

   Der Assistent für das Erstellen eines autonomen Installationspakets wird geschlossen.

Das autonome Installationspaket wird im Unterordner PkgInst des Freigegebenen Ordners des Administrationsservers erstellt und abgelegt. Sie können eine Liste der autonomen Pakete anzeigen. Klicken Sie dazu oberhalb der Liste der Installationspakete auf **Liste der autonomen Pakete anzeigen**.

Liste der autonomen Installationspakete anzeigen

Sie können die Liste der autonomen Installationspakete und die Eigenschaften jedes der autonomen Installationspakete anzeigen.

So zeigen Sie die Liste der autonomen Installationspakete für alle Installationspakete an:

Klicken Sie oberhalb der Liste auf die Schaltfläche **Liste der autonomen Pakete anzeigen**.

In der Liste der autonomen Installationspakete werden deren Eigenschaften wie folgt angezeigt:

- **Paketname**. Name des autonomen Installationspaketes, der automatisch aus dem Namen der im Paket enthaltenen Anwendung und der Anwendungsversion gebildet wird.
- **Programmname**. Name der Anwendung, die in dem autonomen Installationspaket enthalten ist.
- **Programmversion**.
- **Installationspaket-Name des Administrationsagenten**. Diese Eigenschaft wird nur angezeigt, wenn in dem autonomen Installationspaket der Administrationsagent enthalten ist.
- **Version des Administrationsagenten**. Diese Eigenschaft wird nur angezeigt, wenn in dem autonomen Installationspaket der Administrationsagent enthalten ist.
- **Größe**. Dateigröße (MB).
- **Gruppe**. Name der Gruppe, in die das Client-Gerät nach der Installation des Administrationsagenten verschoben wird.
- **Erstellt**. Datum und Uhrzeit der Erstellung des autonomen Installationspakets.
- **Geändert**. Datum und Uhrzeit der Änderung des autonomen Installationspakets.
- **Pfad**. Vollständiger Pfad des Ordners, in dem sich das autonome Installationspaket befindet.

- **Webadresse**. Webadresse des Speicherorts für das autonome Installationspaket.
- **Dateihash**. Mit dieser Eigenschaft wird bestätigt, dass das autonome Installationspaket nicht von Dritten geändert wurde und der Benutzer dieselbe Datei erhalten hat, die Sie erstellt und an den Benutzer übertragen haben.

So zeigen Sie die Liste der autonomen Installationspakete für ein bestimmtes Installationspaket an:

Wählen Sie in der Liste das Installationspaket aus und klicken Sie auf die Schaltfläche **Liste der autonomen Pakete anzeigen** über der Liste.

In der Liste der autonomen Installationspakete können Sie Folgendes tun:

- Veröffentlichen eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichen**. Ein veröffentlichtes autonomes Installationspaket kann von jenen Benutzern heruntergeladen werden, denen Sie einen Link für dieses autonome Installationspaket geschickt haben.
- Aufheben der Veröffentlichung eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichung aufheben**. Ein unveröffentlichtes autonomes Installationspaket kann nur von Ihnen selbst und von anderen Administratoren heruntergeladen werden.
- Herunterladen eines autonomen Installationspakets auf Ihr Gerät, indem Sie auf die Schaltfläche **Herunterladen** klicken.
- Senden einer E-Mail-Nachricht mit einem Link für das autonome Installationspaket durch Klick auf **Per E-Mail senden**.
- Löschen Sie ein autonomes Installationspaket, indem Sie auf die Schaltfläche **Entfernen** klicken.

Erstellen benutzerdefinierter Installationspakete

Mit benutzerdefinierten Installationspaketen können Sie die folgenden Aufgaben ausführen:

- Um eine beliebige Anwendung (wie einen Text-Editor) auf einem Client-Gerät zu installieren, beispielsweise mithilfe einer Aufgabe.
- Zum Erstellen eines autonomen Installationspakets.

Ein benutzerdefiniertes Installationspaket ist ein Ordner mit einem Satz von Dateien. Die Quelle, aus der ein benutzerdefiniertes Installationspaket erstellt wird, ist eine *Archivdatei*. Die Archivdatei enthält eine Datei oder mehrere Dateien, die in das benutzerdefinierte Installationspaket aufgenommen werden müssen. Wenn Sie ein benutzerdefiniertes Installationspaket erstellen, können Sie Befehlszeilenparameter angeben, z. B. um das Programm im Silent-Modus zu installieren.

Wenn Sie einen aktiven Lizenzschlüssel für das Schwachstellen- und Patch-Management besitzen, können Sie Ihre standardmäßigen Installationseinstellungen für das entsprechende benutzerdefinierte Installationspaket konvertieren und die von den Kaspersky-Experten empfohlenen Werte verwenden. Die Einstellungen werden nur dann während der Erstellung des benutzerdefinierten Installationspaketes automatisch konvertiert, wenn die dazugehörige ausführbare Datei in der Kaspersky-Datenbank für Drittherstellersoftware enthalten ist.

So erstellen Sie ein benutzerdefiniertes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für neue Installationspakete wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie die Option **Installationspaket aus einer Datei erstellen** aus.

4. Geben Sie den Namen des Pakets an und klicken Sie auf die Schaltfläche **Durchsuchen**.

   In Ihrem Browser wird das Windows-Standardfenster **Öffnen** geöffnet. Dort können Sie eine Datei zum Erstellen des Installationspakets auswählen.

5. Wählen Sie eine Archivdatei aus, die sich auf einem verfügbaren Datenträger befindet.

   Sie können eine Archivdatei zip-, cab-, tar- oder tar.gz-Format hochladen. Es ist nicht möglich, ein Installationspaket aus einer sfx-Datei (selbstextrahierendes Archiv) zu erstellen.

   > Wenn Sie möchten, dass die Einstellungen während der Paketinstallation konvertiert werden, vergewissern Sie sich, dass das Kontrollkästchen **Die Einstellungen der von Kaspersky Security Center erkannten Programme nach Abschluss des Assistenten zu empfohlenen Werten konvertieren** aktiviert ist, und klicken Sie **Weiter**.

   Das Hochladen der Datei auf den Kaspersky Security Center Administrationsserver wird gestartet.

   > Wenn Sie die Verwendung von empfohlenen Installationseinstellungen aktiviert haben, prüft Kaspersky Security Center 15.1, ob die ausführbare Datei in der Kaspersky-Datenbank für Drittanbieter-Anwendungen enthalten ist. Bei erfolgreicher Prüfung erhalten Sie einen Hinweis, dass die Datei erkannt wurde. Die Einstellungen werden konvertiert und das benutzerdefinierte Installationspaket wird erstellt. Es sind keine weiteren Aktionen erforderlich. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Assistenten zu schließen.

6. Wählen Sie eine Datei aus (von der Liste der Dateien, die aus der ausgewählten Archivdatei extrahiert wurden) und geben Sie die Befehlszeilenparameter einer ausführbaren Datei an.

   Sie können bestimmte Befehlszeilenparameter angeben, um die Anwendung im Silent-Modus aus dem Installationspaket zu installieren. Die Angabe von Befehlszeilenparametern ist optional.

   Das Erstellen des Installationspakets wird gestartet.

   Der Assistent meldet, wenn der Vorgang abgeschlossen ist.

Falls das Installationspaket nicht erstellt wurde, wird eine entsprechende Meldung angezeigt.

7. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Assistenten zu schließen.

Das von Ihnen erstellte Installationspaket wird in den Unterordner "Pakete" des Freigegebenen Ordners des Administrationsservers heruntergeladen. Nach dem Herunterladen erscheint das Installationspaket in der Liste der Installationspakete.

Wenn Sie in der Liste der Installationspakete, die auf dem Administrationsserver verfügbar sind, auf den Link mit dem Namen eines benutzerdefinierten Installationspakets klicken, können Sie:

- Anzeigen der folgenden Eigenschaften eines Installationspakets:
  - **Name**. Der Name des benutzerdefinierten Installationspakets.
  - **Quelle**. Der Hersteller der Anwendung.
  - **Programm**. Die im benutzerdefinierten Installationspaket enthaltene Anwendung.
  - **Version**. Version der Anwendung.
  - **Sprache**. Sprache der Anwendung, die im benutzerdefinierten Installationspaket enthalten ist.
  - **Größe (MB)**. Größe des Installationspakets.
  - **Betriebssystem**. Typ des Betriebssystems, für welches das Installationspaket vorgesehen ist.
  - **Erstellt**. Erstellungsdatum des Installationspakets.
  - **Geändert**. Änderungsdatum des Installationspaketes.
  - **Typ**. Typ des Installationspakets.
- Paketname und Befehlszeilenparameter ändern. Diese Funktion ist nur für Pakete verfügbar, die nicht auf Basis von Kaspersky-Anwendungen erstellt wurden.

Wenn Sie für den Erstellungsprozess des benutzerdefinierten Pakets die Einstellungen des Installationspakets in die empfohlenen Werte konvertiert haben, können Ihnen in den Einstellungen des benutzerdefinierten Installationspakets auf der Registerkarte **Einstellungen** zwei zusätzliche Abschnitte angezeigt werden: **Einstellungen** und **Installationsreihenfolge**.

Der Abschnitt **Einstellungen** enthält die folgenden, tabellarisch aufgeführten Eigenschaften:

- **Name**. Die Spalte gibt den dem Installationsparameter zugewiesen Namen an.
- **Typ**. Die Spalte gibt den Typ des Installationsparameters an.
- **Wert**. Die Spalte gibt den durch den Installationsparameter definierten Datentyp an (Bool, Filepath, Numeric, Path oder String).

Der Abschnitt **Installationsreihenfolge** enthält eine Tabelle, welche die folgenden Eigenschaften von dem Update angibt, das im benutzerdefinierten Installationspaket enthalten ist:

- **Name**. Der Name des Updates.
- **Beschreibung**. Die Beschreibung des Updates.
- **Quelle**. Die Quelle des Updates, d. h. entweder von Microsoft oder von einem anderen Dritthersteller veröffentlicht.
- **Typ**. Der Typ des Updates, d. h. entweder für einen Treiber oder für ein Programm vorgesehen.
- **Kategorie**. Die für Microsoft-Updates angegebene Kategorie des Windows Server Update-Dienstes (WSUS) (Kritische Updates, Definitionsupdates, Treiber, Funktionspakete, Sicherheitsupdates, Servicepakete, Tools, Update-Rollups, Updates, oder Upgrades).
- **Ereigniskategorie entsprechend MSRC**. Die durch das Microsoft Security Response Center (MSRC) definierte Ereigniskategorie des Updates.
- **Ereigniskategorie**. Die durch Kaspersky definierte Ereigniskategorie des Updates.
- **Ereigniskategorie des Patches (für Patches, die für Kaspersky-Anwendungen vorgesehen sind)**. Die Ereigniskategorie eines Patches, wenn dieser für eine Kaspersky-Anwendung vorgesehen ist.
- **Artikel**. Die ID des Artikels, welcher das Update beschreibt, in der Wissensdatenbank.
- **Bulletin**. Die ID des Security-Bulletins, welches das Update beschreibt.
- **Nicht zur Installation zugewiesen**. Gibt an, ob das Update den Status "Nicht zur Installation zugewiesen" besitzt.
- **Zur Installation**. Gibt an, ob das Update den Status "Zur Installation" besitzt.
- **Installation**. Gibt an, ob das Update den Status "Installation" besitzt.
- **Installiert**. Gibt an, ob das Update den Status "Installiert" besitzt.
- **Fehlgeschlagen**. Gibt an, ob das Update den Status "Fehlgeschlagen" besitzt.
- **Neustart erforderlich**. Gibt an, ob das Update den Status "Neustart erforderlich" besitzt.
- **Registriert**. Gibt Datum und Uhrzeit an, wann das Update registriert wurde.
- **Installation im interaktiven Modus**. Gibt an, ob das Update während der Installation Benutzerinterkation erfordert.
- **Widerrufen**. Gibt Datum und Uhrzeit an, wann das Update widerrufen wurde.
- **Genehmigungsstatus des Updates**. Gibt an, ob das Update zur Installation genehmigt wurde.
- **Revision**. Gibt die aktuelle Revisionsnummer des Updates an.
- **Update-ID**. Gibt die Update-ID an.
- **Programmversion**. Gibt die Versionsnummer an, auf welche das Programm aktualisiert wird.

- **Ersetzt**. Gibt ein oder mehrere andere Updates an, die dieses Update ersetzen können.
- **Ersetzend**. Gibt ein oder mehrere Updates an, die durch dieses Update ersetzt werden können.
- **Sie müssen die Bedingungen des Lizenzvertrags akzeptieren**. Gibt an, ob das Update das Akzeptieren des Endbenutzer-Lizenzvertrags (EULA) erfordert.
- **Hersteller**. Gibt den Namen des Herstellers des Updates an.
- **Programmfamilie**. Gibt den Namen der Programmfamilie an, zu welcher dieses Update gehört.
- **Programm**. Gibt den Namen des Programms an, zu welchem dieses Update gehört.
- **Sprache**. Gibt die Sprache der Update-Lokalisierung an.
- **Nicht zur Installation zugewiesen (neue Version)**. Gibt an, ob das Update den Status "Nicht zur Installation zugewiesen (neue Version)" besitzt.
- **Erfordert vorbereitende Installation**. Gibt an, ob das Update den Status "Erfordert vorbereitende Installation" besitzt.
- **Download-Modus**. Gibt den Modus des Update-Downloads an.
- **Ist ein Patch**. Gibt an, ob das Update ein Patch ist.
- **Nicht installiert**. Gibt an, ob das Update den Status "Nicht installiert" besitzt.

Installationspakete an sekundäre Administrationsserver verteilen

Kaspersky Security Center ermöglicht Ihnen das erstellen von Installationspaketen für Kaspersky-Anwendungen und für Anwendungen von Drittanbietern. Darüber hinaus können Sie die Installationspakete an Client-Geräte verteilen und Anwendungen aus den Paketen installieren. Um die Auslastung des primären Administrationsservers zu optimieren, können Sie Installationspakete auf sekundäre Administrationsserver verteilen. Danach übertragen die sekundären Server die Pakete an die Client-Geräte, und anschließend können Sie die Remote-Installation der Anwendungen auf Ihren Client-Geräten durchführen.

Um Installationspakete auf sekundäre Administrationsserver zu verteilen:

1. Stellen Sie sicher, dass die sekundären Administrationsserver mit dem primären Administrationsserver verbunden sind.
2. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

   Die Aufgabenliste wird angezeigt.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
4. Wählen Sie auf der Seite **Einstellungen der neue Aufgabe** in der Dropdown-Liste **Programm** die Option **Kaspersky Security Center**. Wählen Sie anschließend von der Dropdown-Liste **Aufgabentyp** die Option **Installationspaket verteilen** aus und geben Sie den Aufgabennamen an.

5. Wählen Sie auf der Seite **Gültigkeitsbereich der Aufgabe** die Geräte aus, denen die Aufgabe auf folgende Arten zugewiesen ist:

   - Wenn Sie eine Aufgabe für alle sekundären Administrationsserver einer bestimmten Administrationsgruppe erstellen möchten, wählen Sie diese Gruppe aus und erstellen Sie anschließend eine Gruppenaufgabe für sie.

   - Wenn Sie eine Aufgabe für bestimmte sekundäre Administrationsserver erstellen möchten, wählen Sie diese Server aus und erstellen Sie anschließend eine Aufgabe für diese.

6. Wählen Sie auf der Seite **Verteilte Installationspakete** die Installationspakete aus, die auf die sekundären Administrationsserver kopiert werden sollen.

7. Geben Sie ein Konto an, unter dem die Aufgabe *Installationspaket verteilen* ausgeführt wird. Sie können Ihr Konto verwenden und die Option **Standardbenutzerkonto** aktiviert lassen. Alternativ können Sie angeben, dass die Aufgabe unter einem anderen Konto ausgeführt werden soll, welches über die erforderlichen Zugriffsrechte verfügt. Wählen Sie dazu die Option **Benutzerkonto festlegen** aus und geben Sie anschließend die Anmeldeinformationen für dieses Konto ein.

8. Auf der Seite **Erstellung der Aufgabe abschließen** können Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, um anschließend das Fenster mit den Aufgabeneigenschaften zu öffnen und die Aufgabeneinstellungen zu ändern. Alternativ können Sie Aufgabeneinstellungen jederzeit später konfigurieren.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Die Aufgabe, die zur Verteilung der Installationspakete an die sekundären Administrationsserver erstellt wurde, wird in der Aufgabenliste angezeigt.

10. Sie können die Aufgabe manuell starten oder warten, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Aufgabe werden die ausgewählten Installationspakete auf die angegebenen sekundären Administrationsserver kopiert.

Programme mit der Aufgabe zur Remote-Installation installieren

Kaspersky Security Center ermöglicht es, Programme auf den Geräten per Remote-Zugriff mithilfe der Aufgaben der Remote-Installation zu installieren. Mithilfe des Assistenten werden die Aufgaben erstellt und den Geräten zugewiesen. Um den Geräten schneller und einfacher eine Aufgabe zuzuweisen, können Sie die (bis zu 1.000) Geräte im Fenster des Assistenten auf die von Ihnen bevorzugte Art festlegen:

- **Geräte auswählen, die vom Administrationsserver erkannt wurden**. In diesem Fall wird die Aufgabe einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

- **Geräteadressen manuell angeben oder aus Liste importieren**. Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

- **Aufgabe einer Geräteauswahl zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine vordefinierte Auswahl oder Ihre eigene Auswahl angeben.

- **Aufgabe einer Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Administrationsgruppe gehören.

Um Probleme zu vermeiden, die während der Installation der Anwendung auf einem Client-Gerät ohne installierten Administrationsagent auftreten können, müssen Sie vorgehen, wie hier beschrieben: Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center.

Eines Programm remote installieren

Dieser Abschnitt enthält Informationen darüber, wie eine Anwendung in einer Administrationsgruppe, auf Geräten mit bestimmten IP-Adressen oder in einer Auswahl verwalteter Geräte per Fernzugriff installiert werden.

Um eine Anwendung auf ausgewählten Geräten zu installieren:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Feld **Aufgabentyp** die Variante **Remote-Installation eines Programms** aus.
4. Wählen Sie eine der folgenden Varianten aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

     Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

   Die Aufgabe *Remote-Installation einer Anwendung* wird für die angegebenen Geräte erstellt. Wenn Sie Option **Aufgabe einer Administrationsgruppe zuweisen** ausgewählt haben, ist die Aufgabe eine Gruppenaufgabe.
5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

   Die verfügbaren Einstellungen hängen von der im vorherigen Schritt ausgewählten Option ab.

6. Geben Sie im Schritt **Installationspakete** die folgenden Einstellungen an:

- Wählen Sie im Feld **Installationspaket auswählen** das Installationspaket einer Anwendung, die Sie installieren möchten.

- Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Programminstallation erforderlichen Dateien auf die Client-Geräte aus:

  - **Unter Nutzung des Administrationsagenten**

    Wenn die Option aktiviert ist, werden die Installationspakete von dem auf den Client-Geräten installierten Administrationsagenten zugestellt.

    Wenn diese Option deaktiviert ist, werden Installationspakete mithilfe der Betriebssystems-Tools der Client-Geräte ausgeliefert.

    Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

    Diese Option ist standardmäßig aktiviert.

  - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**

    Wenn diese Option aktiviert ist, werden Installationspakete mithilfe der Tools von den Betriebssystemen durch Verteilungspunkte auf die Geräte übertragen. Diese Variante ist wählbar, wenn sich im Netzwerk mindestens ein Verteilungspunkt befindet.

    Ist die Option **Mithilfe des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Betriebssystem-Tools zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

    Standardmäßig ist diese Option für die Aufgaben von Remote-Installationen aktiviert, die auf einem virtuellen Administrationsserver erstellt wurden.

    > Wenn alle Verteilungspunkte, die einem Gerät zugewiesen wurden, fehlerhaft sind, erhält das Gerät keine Updates (Antiviren-Datenbanken und Patches) und keine Installationspakete.

  - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**

    Wenn diese Option aktiviert ist, werden die Dateien durch den Administrationsserver mittels Betriebssystem-Tools der Client-Gerät auf die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

    Diese Option ist standardmäßig aktiviert.

- Geben Sie im Feld **Maximale Anzahl gleichzeitiger Downloads** die erlaubte Maximalanzahl an Client-Geräten, an die der Administrationsserver simultan Dateien ausliefern kann.

- Geben Sie im Feld **Maximale Anzahl der Installationsversuche** die maximal zulässige Anzahl von gestarteten Installationsvorgängen an.

  Wenn die im Parameter angegebene Anzahl an Versuchen überschritten wird, startet Kaspersky Security Center das Installationsprogramm auf dem Gerät nicht mehr. Um die Aufgabe *Remote-Installation einer Anwendung* erneut zu starten, erhöhen Sie den Wert für den Parameter **Maximale Anzahl der Installationsversuche** und starten Sie die Aufgabe erneut. Alternativ dazu können Sie eine neue Aufgabe zur *Remote-Installation einer Anwendung* erstellen.

- Wenn Sie von einer Kaspersky-Sicherheitsanwendung auf eine andere migrieren möchten und die aktuelle Anwendung durch ein Kennwort geschützt ist, geben Sie das Kennwort in dem Feld **Kennwort zur Deinstallation der aktuellen Kaspersky-Anwendung** ein Beachten Sie, dass Ihre aktuelle Kaspersky-Anwendung während der Migration deinstalliert wird.

  Das Feld **Kennwort zur Deinstallation der aktuellen Kaspersky-Anwendung** ist nur verfügbar, wenn Sie die Option **Unter Nutzung des Administrationsagenten** in der Einstellungsgruppe **Download des Installationspakets erzwingen** ausgewählt haben.

  Sie können das Deinstallationskennwort nur für das Migrationsszenario von Kaspersky Security für Windows Server auf Kaspersky Endpoint Security für Windows verwenden, wenn Sie Kaspersky Endpoint Security für Windows mithilfe der Aufgabe zur Remote-Installation von Programmen installieren. Die Verwendung des Deinstallationskennworts bei der Installation anderer Komponenten kann zu Installationsfehlern führen.

  Um das Migrationsszenario erfolgreich abzuschließen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

  - Sie verwenden Kaspersky Security Center Administrationsagent 14.2 für Windows oder höher.
  - Sie installieren das Programm auf Geräten mit Microsoft Windows.

- Passen Sie die erweiterte Einstellung an:

  - **Anwendung nicht neu installieren, wenn sie bereits installiert ist**

    Wenn diese Option aktiviert ist, wird die ausgewählte Anwendung nicht neu installiert, wenn es bereits auf dem Client-Gerät installiert ist.

    Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Anwendung in jedem Fall installiert.

    Diese Option ist standardmäßig aktiviert.

  - **Typ des Betriebssystems vor dem Download prüfen**

    Bevor die Dateien auf die Client-Geräte übertragen werden, prüft Kaspersky Security Center, ob die Einstellungen des Installationstools auf dem Betriebssystem des Client-Geräts anwendbar sind. Wenn die Einstellungen nicht anwendbar sind, überträgt Kaspersky Security Center die Dateien nicht und wird nicht versuchen, die Anwendung zu installieren. So können Sie beispielsweise eine Anwendung auf den Geräten einer Administrationsgruppe, die mehrere Geräte mit unterschiedlichen Betriebssystemen enthält, installieren, indem Sie die Aufgabe zur Installation der Administrationsgruppe zuweisen und anschließend die Option zum Überspringen von Geräten mit davon abweichenden Betriebssystemen aktivieren.

    Wenn Sie den Administrationsagenten per Remote-Installation auf nicht zugeordneten Geräten installieren, bestimmt Kaspersky Security Center oder ein Verteilungspunkt das Betriebssystem des Geräts automatisch, unabhängig davon, welchen Wert die Einstellung **Typ des Betriebssystems vor dem Download prüfen** hat.

  - **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen**

    Wenn diese Option aktiviert ist, wird das Installationspaket mithilfe von Richtlinien des Active Directory installiert.

    Die Option ist verfügbar, wenn ein Installationspaket des Administrationsagenten ausgewählt ist.

    Diese Option ist standardmäßig deaktiviert.

- **Benutzer auffordern, laufende Programme zu schließen**

  Laufende Anwendungen können das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

- Wählen Sie aus, auf welchen Geräten Sie die Anwendung installieren möchten:

  - **Auf allen Geräten installieren**

    Wird die Anwendung selbst auf den Geräten installiert, die von anderen Administrationsservern verwaltet werden.

    Diese Variante ist standardmäßig festgelegt. Sie müssen diese Einstellung nicht ändern, wenn Sie nur einen Administrationsserver in Ihrem Netzwerk haben.

  - **Nur auf Geräten installieren, die durch diesen Administrationsserver verwaltet werden**

    Wird die Anwendung nur auf den Geräten installiert, die von diesem Administrationsserver verwaltet werden. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk mehrere Administrationsserver haben und Konflikte zwischen diesen vermeiden möchten.

- Geben Sie an, ob die Geräte nach Abschluss der Installation in eine Administrationsgruppe verschoben werden müssen:

  - **Geräte nicht verschieben**

    Die Geräte bleiben in den Gruppen, in denen sie sich gerade befinden. Die Geräte, die keiner Gruppe zugeordnet wurden, bleiben nicht zugeordnet.

  - **Nicht zugeordnete Geräte in die ausgewählte Gruppe verschieben (es kann nur eine Gruppe ausgewählt werden)**

    Die Geräte werden in die ausgewählte Administrationsgruppe verschoben.

  Beachten Sie, dass die Option **Geräte nicht verschieben** standardmäßig festgelegt ist. Aus Sicherheitsgründen sollten Sie die Geräte manuell verschieben.

7. Geben Sie in diesem Schritt des Assistenten an, ob die Geräte während der Installation von Anwendungen neu gestartet werden sollen:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen nach (Min.)**

    Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

    Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neu starten nach (Min.)**

    Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

    Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

8. Bei Bedarf können Sie im Schritt **Benutzerkonten für den Zugriff auf Geräte auswählen** die Konten hinzufügen, die zum Start der Aufgabe *Remote-Installation eines Programms* verwendet werden sollen:

   - **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

     Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm der Anwendung gestartet werden soll. Die Aufgabe wird unter dem Konto gestartet, unter dem der Dienst des Administrationsservers läuft.

     Wenn der Administrationsagent nicht auf den Client-Geräten installiert ist, steht diese Option nicht zur Verfügung.

- **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**

  Wählen Sie diese Option, wenn auf den Geräten, denen Sie die Aufgabe zur Remote-Installation zuweisen, der Administrationsagent nicht installiert ist. In diesem Fall können Sie ein Benutzerkonto oder ein SSH-Zertifikat angeben, um die Anwendung zu installieren.

  - **Lokales Benutzerkonto**. Wenn Sie diese Variante auswählen, können Sie das Benutzerkonto angeben, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Benutzerkonto** aus, und geben Sie anschließend die Anmeldeinformationen des Benutzerkontos an.

    Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Benutzerkonto existiert, dass über die erforderlichen Rechte auf allen Geräten verfügt, für welche die Aufgabe bestimmt wurde. In diesem Fall werden für den Start der Aufgabe alle hinzugefügten Konten nacheinander von oben nach unten angewandt.

  - **SSH-Zertifikat**. Wenn Sie eine Anwendung auf einem Linux-basierten Client-Gerät installieren möchten, können Sie anstelle eines Benutzerkontos ein SSH-Zertifikat angeben. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **SSH-Zertifikat** aus, und geben Sie anschließend den privaten und den öffentlichen Schlüssel des Zertifikats an.

    Um einen privaten Schlüssel zu generieren, können Sie das Tool "ssh-keygen" verwenden. Beachten Sie, dass die Kaspersky Security Center das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" den Parameter "-m PEM" hinzu. Beispielsweise:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< Benutzer-E-Mail >"
    ```

9. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu beenden.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen, ändern oder bei Bedarf einen Startzeitplan für die Aufgabe konfigurieren.

10. Wählen Sie in der Aufgabenliste die von Ihnen erstellte Aufgabe aus und klicken Sie anschließend auf **Start**.

    Alternativ können Sie warten, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Remote-Installationsaufgabe wurde die ausgewählte Anwendung auf den angegebenen Geräten installiert.

Programme mit Gruppenrichtlinien des Active Directory installieren

Mit Kaspersky Security Center können Sie Kaspersky-Anwendungen auf verwalteten Geräten mithilfe der Gruppenrichtlinien des Active Directory installieren.

Sie können Programme mithilfe der Gruppenrichtlinien des Active Directory nur aus Installationspaketen installieren, die den Administrationsagenten enthalten.

Um ein Programm mithilfe von Active Directory-Gruppenrichtlinien zu installieren:

1. Starten Sie den Assistenten für die Bereitstellung des Schutzes. Folgen Sie den Anweisungen des Assistenten.
2. Aktivieren Sie auf der Seite **Einstellungen für die Aufgabe zur Remote-Installation** des Assistenten für die Bereitstellung des Schutzes die Option **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen**.
3. Aktivieren Sie auf der Seite **Benutzerkonten für den Zugriff auf Geräte auswählen** die Option **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**.
4. Fügen Sie das entweder Benutzerkonto mit Administratorberechtigungen auf dem Gerät, auf dem Kaspersky Security Center installiert ist hinzu, oder das Benutzerkonto, das in der Domänengruppe der Group Policy Creators Owners beinhaltet ist.
5. Gewähren Sie dem ausgewählten Benutzerkonto die Berechtigungen:
   a. Gehen Sie zu **Systemsteuerung → Verwaltung → Verwaltung von Gruppenrichtlinien**.
   b. Klicken Sie auf den Knoten mit dem gewünschten Namen.
   c. Klicken Sie auf den Abschnitt **Delegieren**.
   d. Wählen Sie in der Dropdown-Liste **Berechtigung** die Option **GPOs verlinken** aus.
   e. Klicken Sie auf **Hinzufügen**.
   f. Wählen Sie im neuen Fenster **Benutzer, Computer oder Gruppe auswählen** das gewünschte Benutzerkonto.
   g. Klicken Sie auf **OK**, um das Fenster **Benutzer, Computer oder Gruppe auswählen** zu schließen.
   h. Wählen Sie in der Liste **Benutzer und Gruppen** das Konto, dass Sie gerade hinzugefügt haben und klicken Sie anschließend auf **Erweitert → Erweitert**.
   i. Doppelklicken Sie in der Liste **Berechtigungseinträge** auf das Konto, dass Sie gerade hinzugefügt haben.
   j. Gewähren Sie die folgenden Berechtigungen:
      - **Erstellen von Gruppenobjekten**
      - **Löschen von Gruppenobjekten**
      - **Objekte für Gruppenrichtliniencontainer erstellen**
      - **Objekte für Gruppenrichtliniencontainer löschen**
   k. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.
6. Legen Sie die weiteren Einstellungen fest, indem Sie den Anweisungen des Assistenten folgen.
7. Starten Sie die erstellte Aufgabe zur Remote-Installation manuell oder gemäß einem Zeitplan.

Daraufhin wird die Remote-Installation auf folgende Weise ausgeführt:

1. Nach dem Start der Aufgabe werden in jeder Domäne, zu der Client-Geräte für diese Aufgabe zur Remote-Installation gehören, folgende Objekte angelegt:

   - Group policy object (GPO) mit dem Namen **Kaspersky_AK{GUID}**.

   - Eine Sicherheitsgruppe, die dem GPO entspricht. Diese Sicherheitsgruppe umfasst Client-Geräte, auf die sich die Aufgabe erstreckt. Die Zusammensetzung der Sicherheitsgruppe bestimmt den Geltungsbereich des GPOs.

2. Kaspersky Security Center installiert die Kaspersky-Anwendungen auf den Client-Geräten direkt aus dem freigegeben Netzwerkordner "KLSHARE" der Anwendung. Im Installationsordner von Kaspersky Security Center wird dabei ein untergeordneter Hilfsordner erstellt, der die msi-Datei für das zu installierende Programm enthält.

3. Beim Hinzufügen neuer Geräte zum Gültigkeitsbereich der Aufgabe werden diese erst beim nächsten Start der Aufgabe zur entsprechenden Sicherheitsgruppe hinzugefügt. Wenn die Option **Übersprungene Aufgaben starten** aktiviert ist, werden die Geräte sofort zur Sicherheitsgruppe hinzugefügt.

4. Beim Löschen von Geräten aus dem Gültigkeitsbereich einer Aufgabe werden sie erst beim nächsten Start der Aufgabe aus der Sicherheitsgruppe gelöscht.

5. Beim Löschen einer Aufgabe aus dem Active Directory werden auch das GPO, der Link für das GPO und die entsprechende Sicherheitsgruppe gelöscht.

Wenn Sie ein anderes Installationsschema über Active Directory verwenden möchten, können Sie die Einstellungen manuell ändern. Das kann in folgenden Fällen nötig werden:

- Wenn der Administrator für den Antiviren-Schutz nicht die nötigen Rechte besitzt, um im Active Directory einiger Domänen Änderungen vorzunehmen.

- Wenn das ursprüngliche Installationspaket auf einer separaten Netzwerkressource gespeichert werden soll.

- Wenn ein GPO konkreten Unterabteilungen des Active Directory zugewiesen werden soll.

Folgende alternative Installationsschemata über Active Directory sind verfügbar:

- Falls die Installation direkt aus dem freigegebenen Ordner von Kaspersky Security Center erfolgen soll, muss in den Eigenschaften des GPO eine msi-Datei angegeben werden, die sich im exec-Unterordner des Ordners des Installationspakets für das erforderliche Programm befindet.

- Wenn das Installationspaket in einer anderen Netzwerkressource gespeichert werden muss, kopieren Sie den ganzen Inhalt des Ordners exec in das Paket, weil der Ordner neben der msi-Datei die Konfigurationsdateien enthält, die beim Anlegen des Installationspakets erstellt wurden. Um den Lizenzschlüssel zusammen mit dem Programm zu installieren, kopieren Sie auch die Schlüsseldatei in den Ordner.

Anwendungen auf sekundären Administrationsservern installieren

Um eine Anwendung auf sekundären Administrationsservern zu installieren:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten sekundären Administrationsserver verwaltet.

2. Vergewissern Sie sich, dass sich das zur Anwendung passende Installationspaket auf jedem der gewählten sekundären Administrationsserver befindet. Wenn Sie das Installationspaket auf keinem der sekundären Server finden können, verteilen Sie es. Erstellen Sie dazu eine Aufgabe mit dem Aufgabentyp **Installationspaket verteilen**.

3. Erstellen Sie eine Aufgabe zur Remote-Installation der Anwendung auf den sekundären Administrationsservern. Wählen Sie den Aufgabentyp **Remote-Installation eines Programms auf sekundärem Administrationsserver** aus.

   Der Assistent für das Erstellen einer Aufgabe erstellt eine Aufgabe, mit der die im Assistenten ausgewählte Anwendung per Fernzugriff auf den angegebenen sekundären Administrationsservern installiert werden kann.

4. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Remote-Installationsaufgabe wurde die ausgewählte Anwendung auf den angegebenen sekundären Administrationsservern installiert.

Einstellungen für die Remote-Installation auf Unix-Geräten angeben

Wenn Sie eine Anwendung mithilfe einer Aufgabe zur Remote-Installation auf einem Unix-Gerät installieren, können Sie Unix-spezifische Einstellungen für die Aufgabe angeben. Diese Einstellungen sind in den Aufgabeneigenschaften verfügbar, nachdem die Aufgabe erstellt wurde.

So geben Sie Unix-spezifische Einstellungen für eine Aufgabe zur Remote-Installation an:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf den Namen der Aufgabe zur Remote-Installation, für die Sie die Unix-spezifischen Einstellungen festlegen möchten.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Gehen Sie zu **Programmeinstellungen** → **Unix-spezifische Einstellungen**.

4. Geben Sie die folgenden Einstellungen an:

   - **Legen Sie ein Kennwort für das Root-Benutzerkonto fest (nur für Bereitstellungen mittels SSH)**

     Wenn der Befehl `sudo` auf dem Zielgerät nicht verwendet werden kann, ohne das Kennwort anzugeben, wählen Sie diese Option aus und geben Sie dann das Kennwort für das Root-Benutzerkonto an. Kaspersky Security Center überträgt das Kennwort in verschlüsselter Form an das Zielgerät, entschlüsselt das Kennwort und startet dann im Namen des Root-Benutzerkontos mit dem angegebenen Kennwort den Installationsvorgang.

     > Kaspersky Security Center verwendet das Benutzerkonto oder das angegebene Kennwort nicht, um eine SSH-Verbindung herzustellen.

   - **Geben Sie den Pfad eines auf dem Zielgerät befindlichen temporären Ordners mit Berechtigungen zur Ausführung von Dateien an (nur für Bereitstellungen mittels SSH)**

     Wenn das Verzeichnis /tmp auf dem Zielgerät nicht über die Ausführungsberechtigung verfügt, wählen Sie diese Option aus und geben Sie den Pfad des Verzeichnisses mit der Ausführungsberechtigung an. Kaspersky Security Center verwendet das angegebene Verzeichnis als temporäres Verzeichnis für den Zugriff über SSH. Das Programm legt das Installationspaket in dem Verzeichnis ab und führt den Installationsvorgang aus.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert.

Kaspersky-Anwendung starten und beenden

Mit der Aufgabe *Anwendung starten oder beenden* können Sie Kaspersky-Anwendungen auf verwalteten Geräten starten und beenden.

So erstellen Sie eine Aufgabe zum Starten oder Beenden von Anwendungen:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
3. Wählen Sie in der Dropdown-Liste **Programm** die Anwendung aus, für welche Sie die Aufgabe erstellen möchten.

   In der Liste werden Kaspersky-Anwendungen angezeigt, wenn Sie bereits Verwaltungs-Web-Plug-ins für diese Anwendungen hinzugefügt haben.
4. Wählen Sie in der Liste **Aufgabentyp** die Aufgabe **Programmaktivierung** aus.
5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.

   Der Aufgabenname darf höchstens 100 Zeichen lang sein und darf keine Sonderzeiten ("*<>?\:|) enthalten.
6. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.

7. Gehen Sie im Fenster **Programme** wie folgt vor:

   - Aktivieren Sie die Kontrollkästchen neben den Namen der Anwendungen, für die Sie die Aufgabe erstellen möchten.
   - Wählen Sie die Option **Programm starten** oder **Programm beenden**.

8. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** im Schritt **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

10. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

11. Geben Sie im Fenster mit den Aufgabeneigenschaften die allgemeinen Aufgabeneinstellungen an und speichern Sie anschließend die Einstellungen.

Die Aufgabe wird erstellt und konfiguriert.

Wenn Sie die Aufgabe ausführen möchten, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

Verwaltung mobiler Geräte

Die Verwaltung von mobilen Geräten über Kaspersky Security Center erfolgt mithilfe der Komponente "Verwaltung mobiler Geräte", die eine eigene Lizenz erfordert. Aktivieren und konfigurieren Sie die Komponente "Verwaltung mobiler Geräte", wenn Sie planen, die mobilen Geräte der Mitarbeiter Ihres Unternehmens zu verwalten.

Mit der Komponente "Verwaltung mobiler Geräte" können Sie die Android-Geräte der Mitarbeiter verwalten. Der Schutz wird durch die App Kaspersky Endpoint Security für Android gewährleistet, die auf den Geräten installiert ist. Diese App gewährleistet den Schutz mobiler Geräte vor Web-Bedrohungen, Viren und anderen Programmen, die Bedrohungen darstellen. Für die zentrale Verwaltung über die Kaspersky Security Center Web Console müssen Sie die folgenden Verwaltungs-Plug-in auf dem Gerät installieren, auf dem die Kaspersky Security Center Web Console installiert ist:

- Plug-in von Kaspersky Security für mobile Endgeräte
- Plug-in von Kaspersky Endpoint Security für Android

Weitere Informationen zur Bereitstellung des Schutzes und Verwaltung für mobile Geräte finden Sie in der Hilfe von Kaspersky Security für mobile Endgeräte.

Ändern der Einstellungen für die Verwaltung mobiler Geräte in Kaspersky Security Center Web Console

Um die Einstellungen der Komponente "Verwaltung mobiler Geräte" anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Zusätzliche Ports** aus.

3. Ändern Sie die entsprechenden Einstellungen:

   - **Port für mobile Geräte öffnen**

     Wenn dieser Umschalter aktiviert ist, wird auf dem Administrationsserver der Port für mobile Geräte geöffnet.

     Der Port für mobile Geräte kann nur verwendet werden, wenn die Komponente "Verwaltung mobiler Geräte" installiert wurde.

     Wenn dieser Umschalter deaktiviert ist, wird der Port für mobile Geräte auf dem Administrationsserver nicht verwendet.

     Dieser Umschalter ist standardmäßig deaktiviert.

   - **Port zur Synchronisierung mobiler Geräte**

     Nummer des Ports, der für die Verbindung des mobilen Geräts mit Administrationsserver verwendet wird. Standardmäßig wird Portnummer 13292 verwendet.

     Für die Eingabe wird das Dezimalformat verwendet.

   - **Port zur Aktivierung von mobilen Geräten**

     Port für die Verbindung von Kaspersky Endpoint Security für Android mit den Aktivierungsservern von Kaspersky.

     Standardmäßig wird Portnummer 17100 verwendet.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die mobilen Geräte können jetzt eine Verbindung zum Administrationsserver herstellen.

Ersetzen von Sicherheitsanwendungen von Drittanbietern

Zur Installation der Sicherheitsanwendungen von Kaspersky mithilfe von Kaspersky Security Center ist es möglicherweise erforderlich, Drittanbieter-Programme zu löschen, die mit dem zu installierenden Programm nicht kompatibel ist. Kaspersky Security Center bietet mehrere Methoden zur Deinstallation von Drittanbieter-Programmen.

Inkompatible Programme mittels Installer entfernen

Diese Option ist nur in der Verwaltungskonsole auf Basis der Microsoft Management Console verfügbar.

Die Installationsmethode zum Entfernen inkompatibler Programme wird von verschiedenen Installationsarten unterstützt. Vor der Installation der Sicherheitsanwendungen werden die damit inkompatiblen Programme automatisch gelöscht, wenn im Eigenschaftenfenster des Installationspakets für die Sicherheitsanwendung (Abschnitt **Inkompatible Programme**) die Option **Inkompatible Programme automatisch entfernen** aktiviert ist.

Inkompatible Programme während der Konfiguration der Remote-Installation eines Programms entfernen

Sie können die Option **Inkompatible Programme automatisch entfernen** aktivieren, wenn Sie die Remote-Installation einer Sicherheitsanwendung konfigurieren. In der Verwaltungskonsole auf Basis der Microsoft Management Console (MMC) ist diese Option im Assistenten für Remote-Installationen verfügbar. In der Kaspersky Security Center Web Console finden Sie diese Option im Assistenten für die Bereitstellung des Schutzes. Wenn diese Option aktiviert ist, entfernt Kaspersky Security Center vor der Installation einer Sicherheitsanwendung auf dem verwalteten Gerät inkompatible Programme.

Anleitung:

- Verwaltungskonsole: Inkompatible Programme mit dem Assistenten für Remote-Installationen deinstallieren
- Kaspersky Security Center Web Console: Inkompatible Programme vor der Installation deinstallieren

Löschen der inkompatiblen Programme mithilfe einer separaten Aufgabe

Zum Löschen der inkompatiblen Anwendungen wird die Aufgabe **Remote-Deinstallation der Anwendung** verwendet. Die Aufgabe muss vor der Aufgabe zur Installation der Sicherheitsanwendung auf den Geräten gestartet werden. Beispielsweise kann in der Installationsaufgabe ein Zeitplan des Typs **Nach Beenden einer anderen Aufgabe** ausgewählt werden, wobei die andere Aufgabe die Aufgabe **Remote-Deinstallation der Anwendung** ist.

Die Verwendung dieser Löschmethode ist zweckmäßig, wenn der Installer der Sicherheitsanwendung eines der inkompatiblen Programme nicht erfolgreich löschen kann.

Anleitung für die Verwaltungskonsole: Erstellen einer Aufgabe.

Geräte im Netzwerk finden

In diesem Abschnitt wird die Suche und Entdeckung von Geräten im Netzwerk beschrieben.

Kaspersky Security Center ermöglicht eine Suche der Geräte auf der Grundlage der angegebenen Kriterien. Sie können Suchergebnisse in einer Textdatei speichern.

Mit der Such- und Ermittlungsfunktion können folgende Geräte gefunden werden:

- Verwaltete Geräte der Administrationsgruppen des Kaspersky Security Center Administrationsservers und seiner sekundären Administrationsserver.
- Nicht zugeordnete Geräte, die vom Kaspersky Security Center Administrationsservers und seiner sekundären Administrationsserver verwaltet werden.

Szenario: Netzwerkgeräte finden

Die Gerätesuche muss vor der Installation einer Sicherheitsanwendung ausgeführt werden. Der Administrationsserver erhält Informationen über erkannte Geräte und ermöglicht Ihnen, die Geräte mittels Richtlinien zu verwalten. Regelmäßige Netzwerkabfragen sind erforderlich, um die Liste der im Netzwerk verfügbaren Geräte zu aktualisieren.

Stellen Sie vor dem Start der Netzwerkabfrage sicher, dass das SMB-Protokoll aktiviert ist. Andernfalls kann Kaspersky Security Center die Geräte im abgefragten Netzwerk nicht erkennen. Um das SMB-Protokoll zu aktivieren, folgen Sie der Anleitung für Ihr Betriebssystem.

Die Erkennung von Geräten im Netzwerk erfolgt in den folgenden Schritten:

1. **Geräte entdecken**

   Der Schnellstartassistenten führt Sie durch die erstmalige Gerätesuche und hilft, Geräte im Netzwerk wie z. B. Computer, Tablets und Mobiltelefone zu finden. Die Gerätesuche kann auch manuell durchgeführt werden.

2. **Geplante Abfrage konfigurieren**

   Bestimmen Sie, welche Abfragearten Sie regelmäßig verwenden möchten. Aktivieren Sie die erforderlichen Arten und konfigurieren Sie den Abfragezeitplan. Sie können sich dabei auf die Empfehlungen für die Häufigkeiten von Netzwerkabfragen beziehen.

3. **Regeln zum Hinzufügen neu entdeckter Geräte zu Administrationsgruppen einrichten (optional)**

   Wenn in Ihrem Netzwerk neue Geräte auftauchen, werden sie bei regelmäßigen Abfragen entdeckt und automatisch zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt. Sie können Verschiebungsregeln für Geräte einrichten, um die Zuordnung der Geräte zur Gruppe **Verwaltete Geräte** zu automatisieren. Darüber hinaus können Sie Aufbewahrungsregeln konfigurieren.

   Wenn Sie den Schritt 3 überspringen, werden die neu entdeckten Geräte der Gruppe **Nicht zugeordnete Geräte** zugeordnet. Bei Bedarf können Sie diese Geräte manuell in die Gruppe **Verwaltete Geräte** verschieben. Wenn Sie die Geräte manuell in die Gruppe **Verwaltete Geräte** verschieben, können Sie die Informationen zu jedem Gerät analysieren, bestimmen, ob das Gerät in eine Administrationsgruppe verschoben werden soll, und wenn ja, die entsprechende Gruppe angeben.

Ergebnisse

Der Abschluss des Szenarios bringt folgende Ergebnisse mit sich:

- Der Kaspersky Security Center Administrationsserver findet die Geräte im Netzwerk und stellt Ihnen Informationen zu diesen Geräten zur Verfügung.
- Zukünftige Abfragen werden eingerichtet und nach einem festgelegten Zeitplan ausgeführt.
- Neu entdeckte Geräte werden gemäß den konfigurierten Regeln bestimmten Gruppen zugewiesen. (Falls keine Regeln erstellt wurden, bleiben die Geräte in der Gruppe **Nicht zugeordnete Geräte**).

Suchen von Geräten

Dieser Abschnitt beschreibt die Arten der Gerätesuche, die in Kaspersky Security Center verfügbar sind, und bietet Informationen zur Verwendung jeder dieser Arten.

Der Administrationsserver erhält mittels regelmäßiger Netzwerkabfragen Informationen über die Struktur des Netzwerks und der Geräte in diesem Netzwerk. Diese Informationen werden in der Administrationsserver-Datenbank gespeichert. Der Administrationsserver kann folgende Arten von Netzwerkabfragen durchführen:

- **Windows-Netzwerkabfrage**. Der Administrationsserver kann zwei Arten von Windows-Netzwerkabfragen durchführen: schnell und vollständig. Bei der Schnellabfrage empfängt der Administrationsserver nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks. Während einer vollständigen Abfrage werden zusätzliche Informationen von jedem Client-Gerät abgefragt, z. B. Name des Betriebssystems, IP-Adresse, DNS-Name und NetBIOS-Name. Standardmäßig sind sowohl die Schnellabfrage als auch die vollständige Abfrage aktiviert. Es ist möglich, dass die Windows-Netzwerkabfrage Geräte nicht findet, wenn z. B. die Ports UDP 137, UDP 138, TCP 139 im Router oder durch die Firewall geschlossen sind.

- **Abfrage des Domänencontrollers**. Der Administrationsserver oder ein Verteilungspunkt ruft Informationen über die Domänenstruktur und die DNS-Namen der Geräte ab, die zur Domäne gehören. Diese Art der Abfrage ist standardmäßig aktiviert. Es wird empfohlen, dass Sie die Abfrage von Domänencontrollern verwenden, wenn alle Geräte im Netzwerk Mitglieder einer Domäne sind. Wenn einige der vernetzten Geräte nicht in der Domäne enthalten sind, können diese Geräte mit der Abfrage des Domänencontrollers nicht gefunden werden.

- **IP-Bereiche durchsuchen**. Der Administrationsserver fragt die erstellten IP-Bereiche mittels ICMP-Paketen oder NBNS-Protokoll ab und ruft alle Daten über die Geräte ab, die zu den IP-Bereichen gehören. Diese Art der Abfrage ist standardmäßig deaktiviert. Es wird nicht empfohlen, diese Art der Abfrage zu verwenden, wenn Sie die Windows-Netzwerkabfrage und/oder die Abfrage des Active Directory verwenden.

- **Zeroconf-Abfrage**. Ein Verteilungspunkt, der das IPv6-Netzwerk unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) abfragt. Diese Art der Abfrage ist standardmäßig deaktiviert. Sie können die Zeroconf-Abfrage auf Verteilungspunkten mit Linux verwenden.

Wenn Sie Verschiebungsregeln für Geräte eingerichtet und aktiviert haben, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Verwaltete Geräte** aufgenommen. Wenn keine Verschiebungsregeln aktiviert sind, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Nicht zugeordnete Geräte** aufgenommen.

Sie können die Einstellungen für die Gerätesuche für jede Art separat bearbeiten. Zum Beispiel können Sie den Abfragezeitplan ändern, oder definieren, ob die Domänengesamtstruktur oder nur eine bestimme Domäne abgefragt werden soll.

Stellen Sie vor dem Start der Netzwerkabfrage sicher, dass das SMB-Protokoll aktiviert ist. Andernfalls kann Kaspersky Security Center die Geräte im abgefragten Netzwerk nicht erkennen. Um das SMB-Protokoll zu aktivieren, folgen Sie der Anleitung für Ihr Betriebssystem.

Windows-Netzwerkabfrage

Über die Windows-Netzwerkabfrage

Bei der Schnellabfrage empfängt der Administrationsserver nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks. Bei einer vollständigen Abfrage werden von jedem Client-Gerät folgende Informationen angefordert:

- Betriebssystem-Name
- IP-Adresse
- DNS-Name
- NetBIOS-Name

Die folgenden Voraussetzungen gelten sowohl für die schnelle als auch für die vollständige Abfrage:

- Die Ports UDP 137/138, TCP 139, UDP 445, TCP 445 müssen im Netzwerk verfügbar sein.
- Das SMB-Protokoll ist aktiviert.
- Der Microsoft-Computersuchdienst muss verwendet werden, und der Computer mit dem primären Suchdienst muss auf dem Administrationsserver aktiviert sein.
- Der Microsoft-Computersuchdienst muss verwendet werden, und der Computer mit dem primären Suchdienst muss auf den Client-Geräten aktiviert sein:
  - Auf mindestens einem Gerät, wenn sich nicht mehr als 32 Geräte im Netzwerk befinden.
  - Auf mindestens einem Gerät pro 32 Geräten im Netzwerk.

Die vollständige Abfrage kann nur durchgeführt werden, wenn die Schnellabfrage mindestens einmal durchgeführt wurde.

Einstellungen der Windows-Netzwerkabfrage anzeigen und ändern

Um die Eigenschaften der Windows-Netzwerkabfrage zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Gerätesuche** → **Windows-Domänen**.
2. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster der Windows-Domäneneigenschaften wird geöffnet.
3. Aktivieren oder deaktivieren Sie die Windows-Netzwerkabfrage mit dem Schalter **Abfrage des Windows-Netzwerks aktivieren**.
4. Passen Sie den Abfragezeitplan an. Standardmäßig wird die Schnellabfrage alle 15 Minuten und die vollständige Abfrage alle 60 Minuten ausgeführt.

Varianten für den Zeitplan der Abfrage:

- **Alle n Tage**

  Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

  Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Alle n Minuten**

  Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

- **Nach Wochentagen**

  Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

- **Übersprungene Aufgaben starten**

  Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

  Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

  Diese Option ist standardmäßig deaktiviert.

5. Speichern Sie die Eigenschaften der Windows-Netzwerkabfrage.

Die Eigenschaften werden gespeichert und auf alle entdeckten Windows-Domänen und Arbeitsgruppen angewendet.

Abfrage manuell ausführen

Um die Abfrage sofort auszuführen,

Klicken Sie auf **Schnellabfrage starten** oder **Vollständige Abfrage starten**.

Nach Abschluss der Abfrage können Sie die Liste mit gefundenen Geräten auf der Seite **Windows-Domänen** anzeigen, indem Sie das Kontrollkästchen neben dem Domänennamen auswählen und dann auf die Schaltfläche **Geräte** klicken.

IP-Bereiche abfragen

Ursprünglich erhält Kaspersky Security Center IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts, auf dem es installiert ist. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Security Center das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center fragt alle Adressen von 192.168.0.1 bis 192.168.0.254 ab.

Geben Sie für alle Linux-basierten Hosts innerhalb eines Microsoft Active Directory- oder Samba-Domänencontrollers den `netbios name` und die `workgroup` in der Datei `/etc/samba/smb.conf` an. Andernfalls können Hosts mehrfach in den Abfrageergebnissen enthalten sein.

Kaspersky Security Center kann IP-Bereiche mittels Reverse-DNS-Lookup oder mittels des NBNS-Protokolls abfragen:

- **Reverse-DNS-Lookup**

  Kaspersky Security Center versucht für jede IP-Adresse aus dem festgelegten Bereich eine umgekehrte Namensauflösung zu einem DNS-Namen mithilfe von Standard-DNS-Abfragen durchzuführen. Wenn dieser Vorgang erfolgreich ist, sendet der Server einen `ICMP ECHO REQUEST` (entspricht einem ping-Befehl) an den empfangenen Namen. Wenn das Gerät antwortet, werden die Informationen darüber zur Kaspersky Security Center-Datenbank hinzugefügt. Die umgekehrte Namensauflösung ist erforderlich, um Netzwerkgeräte auszuschließen, die über eine IP-Adresse verfügen können, aber keine Computer sind (Netzwerkdrucker, Router usw.).

  Dieses Abfrageverfahren benötigt einen korrekt konfigurierten DNS-Dienst. Dieser muss über eine Reverse-Lookupzone verfügen. In den Netzwerken, die Active Directory verwenden, wird eine solche Zone automatisch gewartet. In diesen Netzwerken ergibt die IP-Subnetzabfrage jedoch nicht mehr Informationen als die Abfrage des Active Directory. Außerdem wird die Reverse-Lookupzone von Administratoren kleiner Netzwerke oft nicht konfiguriert, da dies für den Betrieb vieler Netzwerkdienste nicht benötigt wird. Aus diesen Gründen ist die IP-Subnetzabfrage standardmäßig deaktiviert.

- **NBNS-Protokoll**

  Wenn die umgekehrte Namensauflösung in Ihrem Netzwerk aus irgendeinem Grund nicht möglich ist, verwendet Kaspersky Security Center das NBNS-Protokoll, um die IP-Bereiche abzufragen. Wenn eine Anfrage an eine IP-Adresse einen NetBIOS-Namen zurückgibt, werden die Informationen zu diesem Gerät der Datenbank von Kaspersky Security Center hinzugefügt.

Stellen Sie vor dem Start der Netzwerkabfrage sicher, dass das SMB-Protokoll aktiviert ist. Andernfalls kann Kaspersky Security Center die Geräte im abgefragten Netzwerk nicht erkennen. Um das SMB-Protokoll zu aktivieren, folgen Sie der Anleitung für Ihr Betriebssystem.

Einstellungen für die Abfrage der IP-Bereiche anzeigen und ändern

Um die Einstellungen für die Abfrage der IP-Bereiche anzuzeigen und zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Gerätesuche** → **IP-Bereiche**.

2. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Eigenschaftenfenster der IP-Abfrage wird geöffnet.

3. Aktivieren oder deaktivieren Sie die IP-Abfrage mit dem Schalter **Abfrage erlauben**.

4. Passen Sie den Abfragezeitplan an. Standardmäßig wird die IP-Abfrage alle 420 Minuten (sieben Stunden) ausgeführt.

   Achten Sie bei der Angabe des Abfrageintervalls darauf, dass diese Angabe den Wert der Lebensdauer der IP-Adresse nicht übersteigt. Wird eine IP-Adresse nicht innerhalb ihrer Lebensdauer durch eine Abfrage verifiziert, wird sie automatisch aus den Abfrageergebnissen entfernt. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden, da dynamische IP-Adressen (mithilfe des DHCP-Protokolls (Dynamic Host Configuration Protocol) zugewiesen) alle 24 Stunden geändert werden.

Varianten für den Zeitplan der Abfrage:

- **Alle n Tage**

  Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

  Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Alle n Minuten**

  Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

- **Nach Wochentagen**

  Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

- **Übersprungene Aufgaben starten**

  Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

  Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

  Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Eigenschaften werden gespeichert und auf alle IP-Bereiche angewendet.

Abfrage manuell ausführen

Um die Abfrage sofort auszuführen,

klicken Sie auf die Schaltfläche **Abfrage starten**.

IP-Bereich hinzufügen und bearbeiten

Ursprünglich erhält Kaspersky Security Center IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts, auf dem es installiert ist. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Security Center das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center fragt alle Adressen von 192.168.0.1 bis 192.168.0.254 ab. Sie können die automatisch festgelegten IP-Bereiche bearbeiten oder eigene IP-Bereiche hinzufügen.

Bereiche können nur für IPv4-Adressen erstellt werden. Wenn Sie die Zeroconf-Abfrage aktivieren, wird Kaspersky Security Center das gesamte Netzwerk abfragen.

Um einen neuen IP-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.
2. Klicken Sie auf **Hinzufügen**, um den neuen IP-Bereich hinzuzufügen.
3. Passen Sie im nächsten Fenster folgende Einstellungen an:
   - **Name des IP-Bereichs**

     Der Name des IP-Bereichs. Sie können den IP-Bereich selbst als Namen angeben, z. B. "192.168.0.0/24".
   - **IP-Intervall oder Subnetzadresse und Maske**

     Legen Sie den IP-Bereich fest, indem Sie entweder die erste und letzte IP-Adresse oder die Subnetzadresse und Subnetzmaske angeben. Sie können auch einen der bereits vorhandenen IP-Bereiche auswählen, indem Sie auf **Durchsuchen** klicken.
   - **Gültigkeitsdauer der IP-Adresse (Stunden)**

     Stellen Sie bei Angabe dieser Einstellung sicher, dass die Lebensdauer das im Abfragezeitplan festgelegte Abfrageintervall übersteigt. Wird eine IP-Adresse nicht innerhalb ihrer Lebensdauer durch eine Abfrage verifiziert, wird sie automatisch aus den Abfrageergebnissen entfernt. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden, da dynamische IP-Adressen (mithilfe des DHCP-Protokolls (Dynamic Host Configuration Protocol) zugewiesen) alle 24 Stunden geändert werden.
4. Wählen Sie **Abfrage des IP-Bereichs zulassen**, wenn Sie das hinzugefügte Subnetz oder den Bereich abfragen möchten. Andernfalls wird das hinzugefügte Subnetz oder der Bereich nicht abgefragt.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Der neue IP-Bereich wird zur Liste mit IP-Bereichen hinzugefügt.

Sie können jeden IP-Bereich separat durchsuchen, indem Sie auf **Abfrage starten** klicken. Nach Abschluss der Abfrage können Sie über die Schaltfläche **Geräte** eine Liste mit entdeckten Geräten anzeigen. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden und entspricht der festgelegten Lebensdauer der IP-Adresse.

Um eine neues Subnetz zu einem vorhandenen IP-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.
2. Klicken Sie auf den Namen des IP-Bereichs, zu dem Sie ein Subnetz hinzufügen möchten.
3. Klicken Sie im folgenden Fenster auf **Hinzufügen**.
4. Geben Sie ein Subnetz an, indem Sie entweder dessen Adresse und Maske oder die erste und letzte IP-Adresse im IP-Bereich verwenden. Sie können auch ein vorhandenes Subnetz hinzufügen, indem Sie auf **Durchsuchen** klicken.
5. Klicken Sie auf die Schaltfläche **Speichern**.

   Das neue Subnetz wird zum IP-Bereich hinzugefügt.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die neuen Einstellungen des IP-Bereichs werden gespeichert.

Sie können beliebig viele Subnetze hinzufügen. Benannte IP-Bereiche dürfen sich nicht überlappen, aber für unbenannte Subnetze innerhalb eines IP-Bereichs gilt keine derartige Beschränkung. Sie können die Abfrage für jeden IP-Bereich unabhängig aktivieren und deaktivieren.

Zeroconf-Abfrage

Diese Art der Abfrage wird nur von Linux-basierten Verteilungspunkten unterstützt.

Ein Verteilungspunkt kann Netzwerke abfragen, die Geräte mit IPv6-Adressen enthalten. In diesem Fall werden keine IP-Bereiche angegeben und der Verteilungspunkt fragt das gesamte Netzwerk unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. Um Zeroconf verwenden zu können, müssen Sie das Tool "avahi-browser" auf dem Verteilungspunkt installieren.

So aktivieren Sie die Abfrage für IPv6-Netzwerke:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.
2. Klicken Sie auf die Schaltfläche **Eigenschaften**.
3. Aktivieren Sie im folgenden Fenster den Umschalter **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden**.

Danach beginnt der Verteilungspunkt das Netzwerk abzufragen. In diesem Fall werden die angegeben IP-Bereiche ignoriert.

Abfrage des Domänencontrollers

Kaspersky Security Center unterstützt die Abfrage eines Microsoft Active Directory-Domänencontrollers und eines Samba-Domänencontrollers.

Kaspersky Security Center ermöglicht die Abfrage eines Samba-Domänen-Controllers nur unter Verwendung eines Linux-Verteilungspunkts. Für einen Samba-Domänencontroller wird Samba 4 als Active Directory-Domänencontroller verwendet.

Wenn Sie einen Domänencontroller abfragen, ruft der Administrationsserver oder ein Verteilungspunkt Informationen über die Domänenstruktur, Benutzerkonten, Sicherheitsgruppen und DNS-Namen jener Geräte ab, die zur Domäne gehören.

Es wird empfohlen, die Abfrage von Domänencontrollern zu verwenden, wenn alle Geräte im Netzwerk Mitglieder einer Domäne sind. Wenn einige der vernetzten Geräte nicht in der Domäne enthalten sind, können diese Geräte mit der Abfrage des Domänencontrollers nicht gefunden werden.

Erforderliche Voraussetzungen

Stellen Sie vor der Abfrage eines Domänencontrollers sicher, dass Sie Verbindungen mit dem Domänencontroller durch eine Firewall oder einen Proxyserver zulassen. Stellen Sie außerdem sicher, dass die folgenden Protokolle auf dem Domänencontroller aktiviert sind:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  Dieses Protokoll wird verwendet, wenn die Verbindung zum Domänencontroller mithilfe der SASL-Authentifizierung hergestellt wird. Der Administrationsserver und die Verteilungspunkte unterstützen nur den Mechanismus DIGEST-MD5.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  Dieses Protokoll wird verwendet, wenn Sie eine verschlüsselte Verbindung zum Domänencontroller herstellen müssen.

Stellen Sie sicher, dass auf dem Gerät des Domänencontrollers die folgenden Ports verfügbar sind:

- 389 für das LDAP-Protokoll und Simple Authentication (einschließlich SASL)
- 636 für das LDAPS-Protokoll

Geben Sie für alle Linux-basierten Hosts innerhalb eines Microsoft Active Directory- oder Samba-Domänencontrollers die Parameter `netbios name` und `workgroup` in der Datei `/etc/samba/smb.conf` an. Andernfalls können Hosts mehrfach in den Abfrageergebnissen enthalten sein.

Wenn eine Domäne von Microsoft Active Directory mehrere Domänencontroller enthält, wird die Auswahl eines bestimmten Controllers während der Domänenabfrage nicht unterstützt. Die Verbindung wird mit dem ersten gefundenen Domänencontroller hergestellt. Um eine ordnungsgemäße Authentifizierung an der Domäne von Microsoft Active Directory sicherzustellen, muss das Feld für den alternativen Antragstellernamen (Subject Alternative Name – SAN) des Zertifikats neben allen Adressen der Domänencontroller, die zu dieser Domäne gehören, auch den NetBIOS-Namen der Domäne von Microsoft Active Directory enthalten.

Abfrage des Domänencontrollers mithilfe des Administrationsservers

Sie können mit dem Administrationsserver nur Microsoft Active Directory-Domänen-Controller abfragen.

So fragen Sie einen Domänencontroller mithilfe des Administrationsservers ab:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → Domänencontroller**.
2. Klicken Sie auf **Abfrage-Einstellungen**.

   Das Fenster **Einstellungen für die Abfrage des Domänencontrollers** wird geöffnet.
3. Wählen Sie die Option **Abfrage des Domänencontrollers aktivieren** aus.

4. Geben Sie im Abschnitt **Erweiterte Einstellungen** den Abfragebereich an:

   - **Aktuelle Domäne abfragen**

     Wählen Sie diese Option, um eine Domäne abzufragen, der Kaspersky Security Center zugehörig ist.

   - **Domänengesamtstruktur abfragen**

     Wählen Sie diese Option, um eine Domänengesamtstruktur abzufragen, der Kaspersky Security Center zugehörig ist.

   - **Angegebene Domänen abfragen**

     Wählen Sie diese Option, um eine Domäne mit der angegebenen Adresse und den Anmeldeinformationen eines Benutzers abzufragen.

5. Geben Sie erforderlichenfalls den Abfragezeitplan an: Das Standardabfrageintervall beträgt eine Stunde. Die alten Daten werden durch die bei der nächsten Abfrage empfangenen Daten vollständig ersetzt.

   Folgende Varianten sind als Intervall verfügbar:

   - **Alle n Tage**

     Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

     Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

   - **Alle n Minuten**

     Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

   - **Nach Wochentagen**

     Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

   - **Monatlich, an angegebenen Tagen der gewählten Wochen**

     Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

   - **Übersprungene Aufgaben starten**

     Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

     Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

     Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

     Diese Option ist standardmäßig deaktiviert.

   Wenn Sie Benutzerkonten in einer Sicherheitsgruppe der Domäne ändern, werden diese Änderungen eine Stunde nach Ihrer Abfrage des Domänencontrollers in Kaspersky Security Center angezeigt.

6. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

7. Wenn Sie die Abfrage sofort durchführen möchten, klicken Sie auf die Schaltfläche **Abfrage starten**.

Abfrage des Domänencontrollers mithilfe eines Verteilungspunkts

Sie können einen Microsoft Active Directory-Domänen-Controller und einen Samba-Domänen-Controller auch mithilfe eines Verteilungspunkts abfragen. Als Verteilungspunkt kann ein verwaltetes Windows- oder Linux-Gerät fungieren.

Für einen Linux-Verteilungspunkt wird die Abfrage eines Microsoft Active Directory-Domänencontrollers und eines Samba-Domänencontrollers unterstützt.
Für einen Windows-Verteilungspunkt wird nur die Abfrage eines Microsoft Active Directory-Domänencontrollers unterstützt.
Die Abfrage mit einem Mac-Verteilungspunkt wird nicht unterstützt.

So konfigurieren Sie die Abfrage von Domänencontrollern mithilfe des Verteilungspunkts:

1. Öffnen Sie die Eigenschaften des Verteilungspunkts.
2. Wählen Sie den Abschnitt **Abfrage des Domänencontrollers** aus.
3. Wählen Sie die Option **Abfrage des Domänencontrollers aktivieren** aus.
4. Wählen Sie den Domänencontroller aus, den Sie abfragen möchten.

   Wenn Sie einen Linux-Verteilungspunkt verwenden, klicken Sie im Abschnitt **Angegebene Domänen abfragen** auf **Hinzufügen** und geben Sie anschließend die Adresse und die Anmeldeinformationen des Domänencontrollers an.

   Wenn Sie einen Windows-Verteilungspunkt verwenden, können Sie eine der folgenden Optionen auswählen:

   - **Aktuelle Domäne abfragen**
   - **Domänengesamtstruktur abfragen**
   - **Angegebene Domänen abfragen**
5. Klicken Sie auf die Schaltfläche **Abfragezeitplan festlegen**, um bei Bedarf die Einstellungen des Abfragezeitplans festzulegen.

   Die Abfrage wird nur entsprechend dem festgelegten Zeitplan gestartet. Das manuelle Starten der Abfrage ist nicht möglich.

Nach Abschluss der Abfrage wird die Domänenstruktur im Abschnitt **Domänencontroller** angezeigt.

Wenn Sie Verschiebungsregeln für Geräte eingerichtet und aktiviert haben, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Verwaltete Geräte** aufgenommen. Wenn keine Verschiebungsregeln aktiviert sind, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Nicht zugeordnete Geräte** aufgenommen.

Die gefundenen Benutzerkonten können für die Domänenauthentifizierung in Kaspersky Security Center Web Console verwendet werden.

Authentifizierung und Verbindung mit einem Domänencontroller

Authentifizierung und Verbindung mit einem Domänencontroller während einer Domänenabfrage

Während der Abfrage eines Domänencontrollers mittels eines Linux-Verteilungspunkts, identifiziert der Verteilungspunkt das Verbindungsprotokoll, um die erstmalige Verbindung mit dem Domänencontroller herzustellen. Dieses Protokoll wird für alle zukünftigen Verbindungen zum Domänencontroller verwendet. Wenn Sie die erste Verbindung mit dem Domänencontroller herstellen, können Sie die Verbindungsoptionen mithilfe der Flags des Administrationsagenten (`KLNAG_LDAP_TLS_REQCERT` und `KLNAG_LDAP_SSL_CACERT`) ändern. Sie können die Flags des Administrationsagenten mithilfe von "klscflag" konfigurieren, wie in diesem Artikel beschrieben.

Die erstmalige Verbindung mit einem Domänencontroller funktioniert wie folgt:

1. Ein Linux-Verteilungspunkt versucht, über LDAPS eine Verbindung mit dem Domänencontroller herzustellen.

   Standardmäßig ist keine Überprüfung des Zertifikats notwendig. Um die Überprüfung des Zertifikats zu erzwingen, setzen Sie das Flag `KLNAG_LDAP_TLS_REQCERT` auf "1".

   Mögliche Einstellungswerte des Parameters `KLNAG_LDAP_TLS_REQCERT`:

   - `0` – Das Zertifikat wird angefordert, aber wenn es nicht bereitgestellt wurde oder die Überprüfung des Zertifikats fehlgeschlagen ist, gilt die TLS-Verbindung dennoch als erfolgreich hergestellt (Standardwert).
   - `1` – Eine strenge Überprüfung des LDAP-Serverzertifikats ist erforderlich.

   Wenn das Flag `KLNAG_LDAP_SSL_CACERT` nicht angegeben ist, wird standardmäßig für den Zugriff auf die Zertifikatskette der vom Betriebssystem abhängige Pfad zur Zertifizierungsstelle (CA) verwendet. Um einen benutzerdefinierten Pfad anzugeben, verwenden Sie das Flag `KLNAG_LDAP_SSL_CACERT`.

2. Wenn die LDAPS-Verbindung fehlschlägt, versucht der Linux-Verteilungspunkt eine Verbindung zum Domänencontroller über eine unverschlüsselte TCP-Verbindung unter Verwendung von SASL (DIGEST-MD5) herzustellen.

Flags konfigurieren

Sie können die Parameter mithilfe des Tools "klscflag" konfigurieren.

Öffnen Sie auf einem Linux-Verteilungspunkt die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Auf einem Linux-Verteilungspunkt befindet sich das klscflag-Tool standardmäßig unter /opt/kaspersky/ksc64/sbin.

Der folgende Befehl erzwingt beispielsweise die Überprüfung des Zertifikats:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Einen Samba-Domänencontroller konfigurieren

Kaspersky Security Center unterstützt nur Linux-Domänencontroller, die auf Samba 4 ausgeführt werden.

Ein Samba-Domänencontroller unterstützt die gleichen Schema-Erweiterungen wie ein Domänencontroller von Microsoft Active Directory. Sie können die vollständige Kompatibilität eines Samba-Domänencontrollers mit einem Microsoft Active Directory-Domänencontroller aktivieren, indem Sie die Samba 4-Schema-Erweiterung verwenden. Dies ist eine optionale Aktion.

Es wird empfohlen, die vollständige Kompatibilität eines Samba-Domänencontrollers mit einem Microsoft Active Directory-Domänencontroller zu aktivieren. Dadurch wird die korrekte Interaktion zwischen Kaspersky Security Center und dem Samba-Domänencontroller gewährleistet.

So aktivieren Sie die vollständige Kompatibilität eines Samba-Domänencontrollers mit einem Microsoft Active Directory-Domänencontroller:

1. Führen Sie den folgenden Befehl aus, um die Schema-Erweiterung "RFC2307" zu verwenden:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Aktivieren Sie auf einem Samba-Domänencontroller das Schema-Update. Fügen Sie dafür der Datei `/etc/samba/smb.conf` die folgende Zeile hinzu:

   ```
   dsdb:schema update allowed = true
   ```

   Wenn das Schema-Update mit einem Fehler abgeschlossen wird, müssen Sie eine vollständige Wiederherstellung jenes Domänencontrollers durchführen, der als Schema-Master agiert.

Geben Sie für alle Linux-basierten Hosts innerhalb eines Samba-Domänencontrollers die Parameter `netbios name` und `workgroup` in der Datei `/etc/samba/smb.conf` an. Andernfalls können Hosts mehrfach in den Abfrageergebnissen enthalten sein.

Aufbewahrungsregeln für nicht zugeordnete Geräte anpassen

Nach Abschluss der Windows-Netzwerkabfrage werden die gefundenen Geräte in Untergruppen der Administrationsgruppe "Nicht zugeordnete Geräte" zusammengefasst. Diese Administrationsgruppe befindet sich unter **Gerätesuche und Bereitstellung** → **Gerätesuche** → **Windows-Domänen**. Der Ordner **Windows-Domänen** ist die übergeordnete Gruppe. Sie enthält untergeordnete Gruppen, die nach den entsprechenden Domänen und Arbeitsgruppen benannt sind, die bei der Abfrage gefunden wurden. Die übergeordnete Gruppe kann auch die Administrationsgruppe für mobile Geräte enthalten. Die Aufbewahrungsregeln für nicht zugeordnete Geräte können für die übergeordnete sowie für jede untergeordnete Gruppe angepasst werden. Die Aufbewahrungsregeln sind nicht von den Einstellungen der Gerätesuche abhängig und sind selbst dann aktiv, wenn die Gerätesuche deaktiviert ist.

Die Geräteaufbewahrungsregeln wirken sich nicht auf Geräte aus, bei denen mindestens ein Laufwerk mittels vollständiger Festplattenverschlüsselung verschlüsselt ist. Solche Geräte werden nicht automatisch gelöscht, sondern können nur manuell gelöscht werden. Wenn Sie ein Gerät löschen wollen, das über ein verschlüsseltes Laufwerk verfügt, entschlüsseln Sie zunächst das Laufwerk und löschen Sie anschließend das Gerät.

Um die Aufbewahrungsregeln für nicht zugeordnete Geräte anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → Windows-Domänen**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf die Schaltfläche **Eigenschaften**, um die Einstellungen der übergeordneten Gruppe anzupassen.

     Das Fenster der Windows-Domäneneigenschaften wird geöffnet.
   - Klicken Sie auf den Namen einer untergeordneten Gruppe, um ihre Einstellungen anzupassen.

     Das Eigenschaftenfenster der untergeordneten Gruppe wird geöffnet.
3. Passen Sie die folgenden Einstellungen an:
   - **Gerät aus Gruppe entfernen, wenn Gerät inaktiv seit (Tagen)**

     Wenn diese Option aktiviert ist, können Sie das Zeitintervall festlegen, nach dem das Geräte automatisch aus der Gruppe gelöscht wird. Standardmäßig wird diese Option auch an die untergeordneten Gruppen weitergegeben. Standardmäßig beträgt das Zeitintervall 7 Tage.

     Diese Option ist standardmäßig aktiviert.
   - **Aus übergeordneter Gruppe erben**

     Wenn diese Option aktiviert ist, wird der Aufbewahrungszeitraum für die Geräte in der aktuellen Gruppe von der übergeordneten Gruppe geerbt und kann nicht geändert werden.

     Diese Option ist nur für untergeordnete Gruppen verfügbar.

     Diese Option ist standardmäßig aktiviert.
   - **Vererbung an untergeordnete Gruppen erzwingen**

     Die Einstellungswerte werden an untergeordnete Gruppen verteilt, aber in den Eigenschaften der untergeordneten Gruppen sind diese Einstellungen gesperrt.

     Diese Option ist standardmäßig deaktiviert.
4. Klicken Sie auf die Schaltfläche **Akzeptieren**.

Ihre Änderungen werden gespeichert und übernommen.

Hardware-Inventur

Die Hardware-Liste (**Vorgänge → Datenverwaltung → Hardware**), die Sie für die Inventur der Hardware verwenden, wird auf zwei Arten gefüllt: automatisch und manuell. Nach jeder Netzwerkabfrage werden alle erkannten Geräte automatisch in die Liste eingetragen. Sie können Geräte aber auch manuell hinzufügen, wenn Sie das Netzwerk nicht abfragen möchten. Sie können manuell weitere Geräte zu der Liste hinzufügen, z. B. Router, Drucker und andere Geräte-Hardware.

In den Eigenschaften eines Geräts können Sie sich ausführliche Informationen über das Gerät anzeigen lassen und diese bearbeiten.

Die Hardware-Liste kann die folgenden Gerätetypen enthalten:

- Computer
- Mobile Geräte
- Netzwerkgeräte
- virtuelle Geräte
- Computer-Hardware (OEM)
- Computer-Peripheriegeräte
- angeschlossene Geräte
- VoIP-Telefonie
- Netzwerkspeicher

Der Administrator kann den gefundenen Geräten das Merkmal *Für Unternehmen* zuweisen. Er kann dieses Merkmal in den Eigenschaften des Geräts manuell zuweisen oder die Kriterien für die automatische Zuweisung festlegen. In diesem Fall wird das Merkmal *Für Unternehmen* nach dem Typ des Geräts zugewiesen.

Kaspersky Security Center ermöglicht es, eine Abschreibung von Hardware durchzuführen. Aktivieren Sie dazu in den Eigenschaften des Geräts die Option **Abgeschrieben**. Ein solches Gerät wird in der Hardware-Liste nicht angezeigt.

Der Administrator kann im Ordner **Hardware** die Liste der speicherprogrammierbaren Steuerungen (SPS) verwenden. Ausführliche Informationen zur Verwendung von SPS-Listen finden Sie im *Benutzerhandbuch für Kaspersky Industrial CyberSecurity for Nodes*.

Informationen über neue Geräte hinzufügen

Um Informationen über neue Geräte hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Hardware**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, um das Fenster **Neues Gerät** zu öffnen.
3. Wählen Sie im Fenster **Neues Gerät** in der Dropdown-Liste **Gerätetyp** den Typ des Gerätes aus, das Sie hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **OK**.

   Das Fenster mit den Geräte-Eigenschaften im Abschnitt **Allgemein** wird geöffnet.

5. Füllen Sie im Abschnitt **Allgemein** die Eingabefelder mit den Daten über das Gerät aus. Im Abschnitt **Allgemein** werden die folgenden Einstellungen angezeigt:

   - **Unternehmensgerät**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie dem Gerät das Merkmal *Für Unternehmen* zuweisen möchten. Nach diesem Merkmal können Sie Suche nach Geräten im Ordner **Hardware** durchführen.

   - **Abgeschrieben**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass das Gerät in der Geräteliste im Ordner **Hardware** angezeigt wird.

6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Das neue Gerät wird im Arbeitsbereich auf der Seite **Hardware** angezeigt.

Kriterien zur Erkennung von Unternehmensgeräten anpassen

Um Kriterien zur Erkennung von Unternehmensgeräten anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Hardware**.

2. Klicken Sie im oberen Bereich der Seite **Hardware** auf den Link **Regel für Geräte mit Merkmal "Unternehmensgerät" einrichten**.

   Der Bereich **Regel für Geräte mit Merkmal "Unternehmensgerät" einrichten** wird aufgerufen.

3. Aktivieren Sie im Bereich **Regel für Geräte mit Merkmal "Unternehmensgerät" einrichten** die Option **Merkmal "Unternehmensgerät" für das Gerät automatisch setzen**. Geben Sie Gerätetypen an, denen das Attribut *Enterprise* automatisch zugewiesen wird.

   > Diese Option wirkt sich nur auf die Geräte aus, die durch Netzwerkabfrage hinzugefügt wurden. Stellen Sie für die manuell hinzugefügten Geräte das Merkmal *Für Unternehmen* manuell ein.

4. Klicken Sie auf die Schaltfläche **OK**.

Die Kriterien zur Bestimmung von Unternehmensgeräte sind konfiguriert.

Anwendungen von Kaspersky: Lizenzierung und Aktivierung

Dieser Abschnitt beschreibt die Funktionen von Kaspersky Security Center, die sich auf die Arbeit mit den Lizenzschlüsseln von verwalteten Kaspersky-Anwendungen beziehen.

Kaspersky Security Center ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Anwendungen auf Client-Geräte sowie die Überwachung der Schlüsselverwendung und die Verlängerung der Gültigkeitsdauer der Lizenz.

Beim Hinzufügen eines Lizenzschlüssels über Kaspersky Security Center werden die Lizenzschlüssel-Einstellungen auf dem Administrationsserver gespeichert. Anhand dieser Informationen erstellt die Anwendung einen Bericht über die Nutzung des Lizenzschlüssels und informiert den Administrator über den Ablauf der Gültigkeitsdauer von Lizenzen und eine Überschreitung der in den Lizenzschlüssel-Einstellungen vorgegebenen Lizenzbeschränkungen. Sie können die Einstellungen für Benachrichtigungen über die Nutzung von Lizenzschlüsseln in den Einstellungen des Administrationsservers konfigurieren.

Lizenzierung der verwalteten Programme

Jedes der auf den verwalteten Geräten installierten Kaspersky-Anwendungen muss mit einer Schlüsseldatei oder einem Aktivierungscode lizenziert werden. Eine Schlüsseldatei oder ein Aktivierungscode kann folgendermaßen bereitgestellt werden:

- Mittels automatischer Verteilung
- Mittels Installationspaket der verwalteten Anwendung
- Mittels *Aufgabe zum Hinzufügen eines Lizenzschlüssels* für ein verwaltetes Programm
- Mittels manueller Aktivierung einer verwalteten Anwendung

Sie können mit einer der oben aufgeführten Methoden einen neuen aktiven Lizenzschlüssel oder einen Reserve-Lizenzschlüssel hinzufügen. Kaspersky-Anwendungen verwenden zum aktuellen Zeitpunkt einen aktiven Schlüssel und speichern einen Reserveschlüssel, der nach Ablauf des aktiven Schlüssels angewendet wird. Die Anwendung, für welche Sie einen Lizenzschlüssel hinzufügen, definiert, ob der Schlüssel aktiv oder reserviert ist. Die Definition des Schlüssels hängt nicht von der Methode ab, die Sie zum Hinzufügen des neuen Lizenzschlüssels verwenden.

Mittels automatischer Verteilung

Wenn Sie verschiedene verwaltete Anwendungen verwenden und eine bestimmte Schlüsseldatei oder Aktivierungscode an die Geräte verteilen möchten, verwenden Sie andere Methoden zur Verteilung des Aktivierungscodes oder der Schlüsseldatei.

Kaspersky Security Center erlaubt die automatische Verteilung der vorhandenen Lizenzschlüssel an die Geräte. Angenommen, in der Datenverwaltung des Administrationsservers befinden sich drei Lizenzschlüssel. Sie haben das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** für alle drei Lizenzschlüssel gewählt. Auf den Unternehmensgeräten ist eine Sicherheitsanwendung von Kaspersky installiert, z. B. Kaspersky Endpoint Security für Windows. Ein neues Gerät wurde entdeckt und erfordert die Bereitstellung eines Lizenzschlüssels. Die Anwendung ermittelt, dass für dieses Gerät z. B. zwei Lizenzschlüssel aus dem Speicher geeignet sind: Lizenzschlüssel *Key_1* und Lizenzschlüssel *Key_2*. Einer dieser Lizenzschlüssel wird an das Gerät verteilt. In diesem Fall kann nicht vorausgesagt werden, welcher der beiden Lizenzschlüssel an das Gerät bereitgestellt werden wird, da die automatische Verteilung von Lizenzschlüsseln keinerlei Aktivitäten des Administrators vorsieht.

Bei der Verteilung des Lizenzschlüssels an das Gerät erfolgt eine Zählung aller Geräte, für die dieser Schlüssel gilt. Sie müssen sicherstellen, dass die Anzahl der Geräte, an die der Lizenzschlüssel verteilt wird, die Lizenzbeschränkung nicht überschreitet. Falls die Anzahl der Geräte die Lizenzbeschränkung überschreitet, wird allen Geräten, die nicht durch die Lizenz abgedeckt sind, der Status *Kritisch* zugewiesen.

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- Verwaltungskonsole:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel automatisch verteilen

  oder
- Kaspersky Security Center Web Console:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel automatisch verteilen

Beachten Sie, dass ein automatisch verteilter Lizenzschlüssel in den folgenden Fällen möglicherweise nicht in der Datenverwaltung des virtuellen Administrationsservers angezeigt wird:

- Der Lizenzschlüssel ist nicht für diese Anwendung vorgesehen.
- Der virtuelle Administrationsserver verfügt über keine verwalteten Geräte.
- Der Lizenzschlüssel wird bereits für Geräte verwendet, die unter Verwaltung eines anderen virtuellen Administrationsservers stehen, und die maximale Anzahl an Geräten wurde erreicht.

Hinzufügen einer Schlüsseldatei oder eines Aktivierungscodes zum Installationspaket einer verwalteten Anwendung

Diese Option wird aus Sicherheitsgründen nicht empfohlen. Eine Schlüsseldatei oder ein Aktivierungscode, der zum Installationspaket hinzugefügt wurde, kann kompromittiert werden.

Wenn die Installation der verwalteten Anwendung mithilfe eines Installationspakets erfolgt, können Sie eine Schlüsseldatei oder einen Aktivierungscode im Installationspaket oder in der Richtlinie dieser Anwendung angeben. Der Lizenzschlüssel wird bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver an die verwalteten Geräte verteilt.

Anleitung:

- Verwaltungskonsole:
  - Installationspaket erstellen
  - Programme auf Client-Geräten installieren

  oder
- Kaspersky Security Center Web Console: Lizenzschlüssel zu einem Installationspaket hinzufügen

Verteilung mithilfe der Aufgabe zum Hinzufügen eines Lizenzschlüssels für ein verwaltetes Programm

Wenn Sie die Aufgabe *Lizenzschlüssel hinzufügen* für verwaltete Programme verwenden, können Sie den Lizenzschlüssel auswählen, der an die Geräte verteilt werden soll, und die Geräte auf die von Ihnen bevorzugte Art auswählen, z. B. indem Sie eine Administrationsgruppe oder eine Geräteauswahl wählen.

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- Verwaltungskonsole:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel auf Client-Geräte verteilen

  oder
- Kaspersky Security Center Web Console:
  - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
  - Lizenzschlüssel auf Client-Geräte verteilen

Manuelles Hinzufügen des Aktivierungscodes oder der Schlüsseldatei auf den Geräten.

Sie können die installierte Kaspersky-Anwendung lokal mittels der Tools in der Programmoberfläche aktivieren. Weitere Informationen finden Sie in der Dokumentation zum installierten Programm.

Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen

Um einen Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie, was Sie hinzufügen möchten:
   - **Schlüsseldatei hinzufügen**

     Klicken Sie auf **Schlüsseldatei auswählen** und finden Sie die .key-Datei, die Sie hinzufügen möchten.

- **Aktivierungscode eingeben**

  Geben Sie im Textfeld den Aktivierungscode an und klicken Sie auf **Senden**.

4. Klicken Sie auf die Schaltfläche **Schließen**.

Der oder die Lizenzschlüssel werden zur Datenverwaltung des Administrationsservers hinzugefügt.

Lizenzschlüssel des Administrationsservers hinzufügen

Um einen Lizenzschlüssel des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Kontextmenü des Administrationsservers **Eigenschaften** aus.
2. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers den Abschnitt **License keys** aus.
3. Klicken Sie im Abschnitt **Aktiver Lizenzschlüssel** auf die Schaltfläche **Bearbeiten**.
4. Fügen Sie im angezeigten Fenster einen Lizenzschlüssel hinzu, indem Sie auf die Schaltfläche **Hinzufügen** klicken.

   Der Add license key wizard wird gestartet.

Nach Abschluss des Assistenten können Sie überprüfen, ob die in der Verwaltungskonsole angezeigten Funktionen denen der zugehörigen Lizenz entsprechen.

Lizenzschlüssel auf Client-Geräte verteilen

Die Kaspersky Security Center Web Console ermöglicht die Verteilung von Lizenzschlüsseln auf Client-Geräte entweder mittels automatischer Verteilung oder mittels der Aufgabe **Programmaktivierung**. Sie können die Aufgabe verwenden, um Schlüssel an eine bestimmte Gerätegruppe zu verteilen. Wenn ein Lizenzschlüssel anhand dieser Aufgabe verteilt wird, werden die Lizenzbeschränkungen für die Anzahl der Geräte nicht berücksichtigt. Verwenden Sie die automatische Verteilung von Schlüsseln, um die Verteilung eines Lizenzschlüssels automatisch einzustellen, wenn die Lizenzbeschränkung erreicht ist.

Wenn Sie die automatische Verteilung eines Lizenzschlüssels aktivieren, erstellen Sie keine Aufgabe des Typs **Programmaktivierung**, um diesen Schlüssel an Client-Geräte zu verteilen. Andernfalls erhöht sich die Belastung des Administrationsservers aufgrund häufiger Synchronisierungen.

Vor der Verteilung müssen Sie den Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen.

*So verteilen Sie einen Lizenzschlüssel an Client-Geräte mittels der Aufgabe **Programmaktivierung**:*

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Wählen Sie in der Dropdown-Liste **Programm** die Anwendung aus, für das Sie einen Lizenzschlüssel hinzufügen möchten.

4. Wählen Sie in der Liste **Aufgabentyp** die Aufgabe **Programmaktivierung** aus.

5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.

6. Wählen Sie die Geräte, denen die Aufgabe zugewiesen werden soll.

7. Klicken Sie im Schritt **Lizenzschlüssel auswählen** des Assistenten auf den Link **Schlüssel hinzufügen**, um den Lizenzschlüssel hinzuzufügen.

8. Fügen Sie im Bereich zum Hinzufügen von Schlüsseln den Lizenzschlüssel mit einer der folgenden Optionen hinzu:

   Sie müssen den Lizenzschlüssel nur dann hinzufügen, wenn Sie ihn vor der Erstellung der Aufgabe **Programmaktivierung** nicht zur Datenverwaltung des Administrationsservers hinzugefügt haben.

   - Wählen Sie die Option **Aktivierungscode eingeben**, um einen Aktivierungscode einzugeben, und gehen Sie anschließend wie folgt vor:

     a. Geben Sie den Aktivierungscode ein und klicken Sie anschließend auf die Schaltfläche **Senden**.

     Die Informationen des Lizenzschlüssels werden im Fenster zum Hinzufügen des Schlüssels angezeigt.

     b. Klicken Sie auf die Schaltfläche **Speichern**.

     Wenn Sie den Lizenzschlüssel automatisch an verwaltete Geräte verteilen möchten, aktivieren Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.

     Der Bereich zum Hinzufügen von Schlüsseln wird geschlossen.

   - Wählen Sie die Option **Schlüsseldatei hinzufügen** aus, um eine Schlüsseldatei hinzuzufügen, und gehen Sie anschließend wie folgt vor:

     a. Klicken Sie auf die Schaltfläche **Schlüsseldatei auswählen**.

     b. Wählen Sie in dem sich öffnenden Fenster eine Schlüsseldatei und klicken Sie anschließend auf die Schaltfläche **Öffnen**.

     Die Informationen des Lizenzschlüssels werden im Fenster zum Hinzufügen des Lizenzschlüssels angezeigt.

     c. Klicken Sie auf die Schaltfläche **Speichern**.

     Wenn Sie den Lizenzschlüssel automatisch an verwaltete Geräte verteilen möchten, aktivieren Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.

     Der Bereich zum Hinzufügen von Schlüsseln wird geschlossen.

9. Wählen Sie in der Tabelle mit Schlüsseln den Lizenzschlüssel aus.

10. Wenn Sie den aktiven Lizenzschlüssel ersetzen möchten, deaktivieren Sie im Schritt **Lizenzinformationen** des Assistenten das standardmäßige Kontrollkästchen **Als Reserveschlüssel verwenden**.

Dies kann beispielsweise erforderlich sein, wenn sich die Organisation ändert und der Schlüssel einer anderen Organisation auf dem Gerät benötigt wird; oder wenn der Schlüssel erneut ausgestellt wurde und eine neue Lizenz früher abläuft als die aktuelle Lizenz. Um Fehler zu vermeiden, müssen Sie das Kontrollkästchen **Als Reserveschlüssel verwenden** deaktivieren.

Weitere Informationen über Probleme, die beim Hinzufügen eines Lizenzschlüssels zu Kaspersky Security Center auftreten können, sowie Möglichkeiten, diese Probleme zu beheben, finden Sie in der Wissensdatenbank von Kaspersky Security Center.

11. Aktivieren Sie beim Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**, um die standardmäßigen Aufgabeneinstellungen zu ändern.

    Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später ändern.

12. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Der Assistent erstellt die Aufgabe. Wenn Sie die Option Nach **Nach Abschluss der Erstellung Aufgabendetails öffnen** haben, wird das Fenster mit Aufgabeneigenschaften automatisch geöffnet. In diesem Fenster können Sie die allgemeinen Aufgabeneinstellungen angeben und bei Bedarf die Einstellungen ändern, die bei der Aufgabenerstellung festgelegt wurden.

    > Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Aufgabenliste auf den Namen der erstellten Aufgabe klicken.

    Die Aufgabe wurde erstellt und konfiguriert und wird in der Aufgabenliste angezeigt.

13. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

    Auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe können Sie auch einen Zeitplan für den Aufgabenstart festlegen.

    Eine detaillierte Beschreibung der Einstellungen für das Starten nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Nachdem dem Abschluss der Aufgabe ist der Lizenzschlüssel auf den ausgewählten Geräten bereitgestellt.

Lizenzschlüssel automatisch verteilen

Kaspersky Security Center ermöglicht das automatische Verteilen von Lizenzschlüsseln, die sich im Schlüsselspeicher auf dem Administrationsserver befinden, auf die verwalteten Geräte.

Um einen Lizenzschlüssel automatisch auf die verwalteten Geräte zu verteilen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge → Lizenzierung → Lizenzen für Kaspersky-Software**.
2. Klicken Sie auf den Namen des Lizenzschlüssels, den Sie automatisch auf die Geräte verteilen möchten.
3. Aktivieren Sie im folgenden Eigenschaftenfenster des Lizenzschlüssels **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Der Lizenzschlüssel wird automatisch an alle kompatiblen Geräte verteilt.

Die Verteilung des Lizenzschlüssels erfolgt durch den Administrationsagenten. Für die Anwendung werden keine Aufgaben zur Verteilung eines Lizenzschlüssels erstellt.

Wenn ein Lizenzschlüssel automatisch verteilt wird, werden die Lizenzbeschränkungen für die Anzahl der Geräte berücksichtigt. Die Beschränkung ist in den Eigenschaften des Lizenzschlüssels festgelegt. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Lizenzschlüssels auf Geräte automatisch beendet.

Beachten Sie, dass ein automatisch verteilter Lizenzschlüssel in den folgenden Fällen möglicherweise nicht in der Datenverwaltung des virtuellen Administrationsservers angezeigt wird:

- Der Lizenzschlüssel ist nicht für diese Anwendung vorgesehen.
- Der virtuelle Administrationsserver verfügt über keine verwalteten Geräte.
- Der Lizenzschlüssel wird bereits für Geräte verwendet, die unter Verwaltung eines anderen virtuellen Administrationsservers stehen, und die maximale Anzahl an Geräten wurde erreicht.

Der virtuelle Administrationsserver verteilt Lizenzschlüssel aus seiner Datenverwaltung und aus der Datenverwaltung des Administrationsservers automatisch. Es wird folgendes Vorgehen empfohlen:

- Verwenden Sie die Aufgabe *Lizenzschlüssel hinzufügen*, um den Lizenzschlüssel auszuwählen, der auf den Geräten verteilt werden soll.
- Vermeiden Sie das Deaktivieren der Option **Automatische Verteilung der Lizenzschlüssel auf die Geräte dieses virtuellen Administrationsservers zulassen** in den Einstellungen des virtuellen Administrationsservers. Andernfalls verteilt der virtuelle Administrationsserver keine Lizenzschlüssel an die Geräte (auch nicht jene Lizenzschlüssel, die sich in der Datenverwaltung des Administrationsservers befinden).

Wenn Sie in dem Eigenschaftenfenster des Lizenzschlüssels das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** auswählen, wird sofort ein Lizenzschlüssel in Ihrem Netzwerk verteilt. Wenn Sie diese Option nicht auswählen, können Sie später eine Aufgabe zur Verteilung der Lizenzschlüssel verwenden.

Die auf dem primären Administrationsserver konfigurierte automatische Verteilung von Lizenzschlüsseln berücksichtigt keine Geräte, die durch nicht-virtuelle sekundäre Administrationsservern verwaltet werden.

Informationen zu verwendeten Lizenzschlüsseln anzeigen

Um die Liste mit Lizenzschlüsseln anzuzeigen, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden, gehen Sie wie folgt vor:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.

Die angezeigte Liste enthält die Schlüsseldatei und Aktivierungscodes, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden.

Um detaillierte Informationen über einen Lizenzschlüssel anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.
2. Klicken Sie auf den Namen des gewünschten Lizenzschlüssels.

Im Eigenschaftenfenster des Lizenzschlüssels können Sie Folgendes ansehen:

- Auf der Registerkarte **Allgemein**: die wichtigsten Informationen über den Lizenzschlüssel
- Auf der Registerkarte **Geräte**: die Liste mit Client-Geräten, auf denen der Lizenzschlüssel für die Aktivierung der installierten Kaspersky-Anwendung verwendet wurde

Um zu sehen, welche Lizenzschlüssel auf einem bestimmten Client-Gerät bereitgestellt werden, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen des gewünschten Geräts.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Programme** aus.
4. Klicken Sie auf den Namen der Anwendung, für das Sie Informationen über den Lizenzschlüssel anzeigen möchten.
5. Wählen Sie im folgenden Fenster mit den Anwendungseigenschaften die Registerkarte **Allgemein** und öffnen Sie dann den Abschnitt **Lizenz**.

Die wichtigsten Informationen über den aktiven Lizenzschlüssel und die Reserveschlüssel werden angezeigt.

Zur Bestimmung der aktuellen Einstellungen für die Lizenzschlüssel des virtuellen Administrationsservers sendet der Administrationsserver mindestens einmal pro Stunde eine Anfrage an die Aktivierungsserver von Kaspersky. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung öffentliche DNS-Server.

Lizenzschlüssel aus der Datenverwaltung entfernen

Wenn Sie einen aktiven Lizenzschlüssel entfernen, der für eine zusätzliche Funktionalität des Administrationsservers wie z. B. Schwachstellen- und Patch-Management oder Verwaltung mobiler Geräte erforderlich ist, ist die entsprechende Funktionalität nicht länger verfügbar. Wenn ein Reserve-Lizenzschlüssel hinzugefügt wurde, wird der Reserve-Lizenzschlüssel automatisch zum aktiven Lizenzschlüssel, nachdem der frühere aktive Lizenzschlüssel entfernt wurde.

Wenn Sie den aktiven Lizenzschlüssel entfernen, der auf einem verwalteten Gerät bereitgestellt wird, bleibt die Anwendung auf dem verwalteten Gerät weiterhin funktionsfähig.

Um eine Schlüsseldatei oder einen Aktivierungscode aus der Datenverwaltung des Administrationsservers zu entfernen, gehen Sie wie folgt vor:

1. Prüfen Sie, dass die Schlüsseldatei oder der Aktivierungscode, den Sie entfernen möchten, nicht vom Administrationsserver verwendet wird. Ein Schlüssel, der vom Administrationsserver verwendet wird, kann nicht entfernt werden. So können Sie dies prüfen:

   a. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

b. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel** aus.

c. Wenn die erforderliche Schlüsseldatei oder der Aktivierungscode in dem geöffneten Abschnitt angezeigt wird, klicken Sie auf die Schaltfläche **Aktiven Lizenzschlüssel entfernen** und bestätigen Sie den Vorgang. Anschließend wird der entfernte Lizenzschlüssel nicht mehr vom Administrationsserver verwendet, befindet sich aber weiterhin in der Datenverwaltung des Administrationsservers. Wird die erforderliche Schlüsseldatei oder der Aktivierungscode nicht angezeigt, so wird er vom Administrationsserver nicht verwendet.

2. Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.

3. Wählen Sie die erforderliche Schlüsseldatei oder den Aktivierungscode aus und klicken Sie anschließend auf die Schaltfläche **Löschen**.

Die ausgewählte Schlüsseldatei oder der Aktivierungscode wird aus der Datenverwaltung entfernt.

Sie können den entfernten Lizenzschlüssel erneut hinzufügen oder einen anderen Lizenzschlüssel hinzufügen.

Vereinbarung mit einem Endbenutzer-Lizenzvertrag widerrufen

Wenn Sie sich entschließen, den Schutz für einige Ihrer Client-Geräte zu beenden, können Sie den Endbenutzer-Lizenzvertrag (EULA) für jede verwaltete Kaspersky-Anwendung widerrufen. Vor dem Widerruf der EULA müssen Sie das ausgewählte Programm deinstallieren.

EULAs, die auf einem virtuellen Administrationsserver akzeptiert wurden, können auf dem virtuellen Administrationsserver und auf dem primären Administrationsserver widerrufen werden. Die EULAs, die auf dem primären Administrationsserver akzeptiert wurden, können nur auf dem primären Administrationsserver widerrufen werden.

So widerrufen Sie eine EULA für verwaltete Kaspersky-Anwendungen:

1. Öffnen Sie das Eigenschaftenfenster des Administrationsservers und wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Endbenutzer-Lizenzverträge**.

   Es wird eine Liste der EULAs angezeigt, die beim Erstellen von Installationspaketen, bei der nahtlosen Installation von Updates oder bei der Bereitstellung von Kaspersky Security für mobile Endgeräte akzeptiert wurden.

2. Wählen Sie in der Liste die EULA aus, die Sie widerrufen möchten.

   Sie können die folgenden Eigenschaften der EULA anzeigen:

   - Datum, an dem die EULA akzeptiert wurde.
   - Name des Benutzers, der die EULA akzeptiert hat.

3. Klicken Sie auf das Datum, an dem die EULA akzeptiert wurde, um ihr Eigenschaftenfenster mit den folgenden Informationen anzuzeigen:

   - Name des Benutzers, der die EULA akzeptiert hat.
   - Datum, an dem die EULA akzeptiert wurde.
   - Eindeutige ID (UID) der EULA.

- Vollständiger Text der EULA.
- Liste der mit der EULA verbundenen Objekte (Installationspakete, nahtlose Updates, Mobile Apps) und ihrer entsprechenden Namen und Typen.

4. Klicken Sie im unteren Teil des EULA-Eigenschaftenfensters auf die Schaltfläche **Lizenzvertrag widerrufen**.

   Sollten Objekte (Installationspakete und ihre entsprechenden Aufgaben) existieren, die den Widerruf der EULA verhindern, wird eine entsprechende Nachricht angezeigt. Sie können den Widerruf erst fortsetzen, wenn Sie diese Objekte gelöscht haben.

   In dem sich öffnenden Fenster werden Sie darüber informiert, dass Sie zunächst die Kaspersky-Anwendung deinstallieren müssen, welches dieser EULA entspricht.

5. Klicken Sie auf die Schaltfläche, um den Widerruf zu bestätigen.

Die EULA wurde widerrufen. Sie wird nicht länger in der Liste der Endbenutzer-Lizenzverträge im Abschnitt **Endbenutzer-Lizenzverträge** angezeigt. Das EULA-Eigenschaftenfenster schließt sich und das Programm ist deinstalliert.

Lizenzen für Kaspersky-Anwendungen verlängern

Lizenzen für Kaspersky-Anwendungen, die entweder abgelaufen oder kurz vor dem Ablaufen sind (weniger als 30 Tage verbleibend) können verlängert werden.

So verlängern Sie Lizenzen, die entweder abgelaufen oder kurz vor dem Ablaufen sind:

1. Führen Sie eine beliebige der folgenden Aktionen aus:
   - Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.
   - Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard** und klicken Sie anschließend auf den Link **Ablaufende Lizenzen anzeigen** neben einer Benachrichtigung.

   Es öffnet sich das Fenster **Lizenzen für Kaspersky-Software**, in dem Sie Lizenzen anzeigen und erneuern können.

2. Klicken Sie neben der erforderlichen Lizenz auf den Link **Lizenz verlängern**.

   Durch Klicken des Links zur Verlängerung der Lizenz erklären Sie sich damit einverstanden, die folgenden Informationen über das Kaspersky Security Center an Kaspersky zu übertragen: die Version, die verwendete Lokalisierung, die ID der Softwarelizenz (d. h. die ID der Lizenz, die Sie verlängern) und ob Sie die Lizenz über ein Partnerunternehmen erworben haben oder nicht.

3. Folgen Sie im sich öffnenden Fensters des Dienstes für Lizenzverlängerung den Anweisungen um eine Lizenz zu verlängern.

   Die Lizenz wird verlängert.

In der Kaspersky Security Center Web Console werden die Benachrichtigungen für eine ablaufende Lizenz entsprechend des folgenden Zeitplans angezeigt:

- 30 Tage vor Ablauf
- 7 Tage vor Ablauf
- 3 Tage vor Ablauf
- 24 Stunden vor Ablauf
- Wenn eine Lizenz abgelaufen ist

Kaspersky Marketplace zum Finden von Kaspersky-Unternehmenslösungen verwenden

Der **Marketplace** ist ein Abschnitt im Hauptmenü, in dem Sie sich das gesamte Angebot an Unternehmenslösungen von Kaspersky anzeigen lassen können, die gewünschten auswählen und anschließend mit dem Kauf auf der Kaspersky-Website fortfahren können. Sie können Filter verwenden, um sich nur die Lösungen anzeigen zu lassen, die zu Ihrem Unternehmen und zu den Anforderungen an Ihr System für Informationssicherheit passen. Wenn Sie eine Lösung auswählen, leitet Sie Kaspersky Security Center auf die entsprechende Webseite innerhalb der Kaspersky-Website weiter, wo Sie mehr über diese Lösung erfahren. Jede Produktseite ermöglicht es Ihnen, mit dem Kauf fortzufahren oder enthält Anweisungen zum Kaufprozess.

Im Abschnitt **Marketplace** können Sie die Lösungen von Kaspersky anhand der folgenden Kriterien filtern:

- Anzahl der Geräte (Endpunkte, Server und andere Arten von Assets), die Sie schützen möchten:
  - 50 – 250
  - 250-1000
  - Über 1000
- Entwicklungsstufe des Informationssicherheitsteams Ihres Unternehmens:
  - **Foundations**

    Diese Stufe ist typisch für Unternehmen, die nur über ein IT-Team verfügen. Die maximal mögliche Anzahl an Bedrohungen wird automatisch blockiert.
  - **Optimum**

    Diese Stufe ist typisch für Unternehmen, die eine bestimmte IT-Sicherheitsfunktion innerhalb des IT-Teams besitzen. Auf dieser Stufe benötigen Unternehmen Lösungen, die es ihnen ermöglichen, sich einfachen Bedrohungen, und Bedrohungen, die bestehende Präventionsmechanismen umgehen, entgegenzustellen.
  - **Expert**

    Diese Stufe ist typisch für Unternehmen mit komplexen und verteilten IT-Umgebungen. Das IT-Sicherheitsteam ist voll entwickelt oder das Unternehmen verfügt über ein eigenes SOC-Team (Security Operations Center). Die benötigten Lösungen ermöglichen es den Unternehmen, komplexen Bedrohungen und gezielten Angriffen zu begegnen.

- Zu schützende Arten von Assets:
  - **Endpunkte**: Workstations von Mitarbeitern, physische und virtuelle Maschinen, Embedded-Systeme
  - **Server**: physische und virtuelle Server
  - **Cloud**: öffentliche, private oder hybride Cloud-Umgebungen sowie Cloud-Dienste
  - **Netzwerk**: lokales Netzwerk, IT-Infrastruktur
  - **Service**: von Kaspersky angebotene sicherheitsbezogene Dienste

So finden und erwerben Sie eine Business-Lösung von Kaspersky:

1. Gehen Sie im Hauptfenster des Menüs zum **Marketplace**.

   Standardmäßig zeigt der Abschnitt alle verfügbaren Business-Lösungen von Kaspersky an.

2. Um nur die Lösungen anzuzeigen, die zu Ihrer Organisation passen, wählen Sie die erforderlichen Werte in den Filtern aus.

3. Klicken Sie auf die Lösung, die Sie kaufen möchten oder über die Sie mehr erfahren möchten.

   Sie werden zur Webseite der Lösung weitergeleitet. Sie können den Anweisungen auf dem Bildschirm folgen, um mit dem Kauf fortzufahren.

Netzwerkschutz konfigurieren

Dieser Abschnitt enthält Informationen über die manuelle Konfiguration von Richtlinien und Aufgaben, über Benutzerrollen und über den Aufbau der Struktur der Administrationsgruppen und der Hierarchie von Aufgaben.

Szenario: Netzwerkschutz konfigurieren

Der Schnellstartassistent erstellt Richtlinien und Aufgaben mit den Standardeinstellungen. Es kann sein, dass diese Einstellungen nicht optimal sind oder in einem Unternehmen als verboten gelten. Deshalb wird empfohlen, die Einstellungen dieser Richtlinien und Aufgaben zu optimieren, und erforderlichenfalls andere Richtlinien und Aufgaben für Ihr Netzwerk zu erstellen.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

- Kaspersky Security Center Administrationsserver installiert haben
- Kaspersky Security Center Web Console installiert haben (optional)
- Das Hauptinstallationsszenario für Kaspersky Security Center abgeschlossen haben

- Der Schnellstartassistent wurde abgeschlossen oder die folgenden Richtlinien und Aufgaben wurden manuell in der Administrationsgruppe **Verwaltete Geräte** erstellt:
  - Richtlinie von Kaspersky Endpoint Security
  - Gruppenaufgabe zum Update von Kaspersky Endpoint Security
  - Richtlinie für den Administrationsagenten
  - Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*

Die Konfiguration des Netzwerkschutzes erfolgt schrittweise:

1. **Einrichtung und Verteilung von Richtlinien und Richtlinienprofilen für Kaspersky-Anwendungen**

   Zur Konfiguration und Verteilung der Einstellungen für auf den verwalteten Geräten installierte Kaspersky-Anwendungen stehen zwei unterschiedliche Methoden der Sicherheitsverwaltung zur Auswahl: die geräteorientierte und die benutzerorientierte Methode. Diese beiden Methoden können auch kombiniert werden. Zur Implementierung einer geräteorientierten Sicherheitsverwaltung können Sie die Werkzeuge nutzen, die von der Microsoft Management Console-basierten Verwaltungskonsole oder von der Kaspersky Security Center Web Console bereitgestellt werden. Die benutzerorientierte Sicherheitsverwaltung kann nur mithilfe der Kaspersky Security Center Web Console erfolgen.

2. **Aufgaben zur Remote-Verwaltung von Kaspersky-Anwendungen konfigurieren**

   Überprüfen Sie die mit dem Schnellstartassistenten erstellten Aufgaben und passen Sie diese bei Bedarf noch feiner an.

   Anleitung:

   - Verwaltungskonsole:
     - Gruppenaufgabe für das Update von Kaspersky Endpoint Security einrichten
     - Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen
   - Kaspersky Security Center Web Console:
     - Gruppenaufgabe für das Update von Kaspersky Endpoint Security einrichten
     - Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates

   Erstellen Sie bei Bedarf zusätzliche Aufgaben, um die auf den Client-Geräten installierten Kaspersky-Anwendungen zu verwalten.

3. **Ereignismenge für Datenbank einschätzen und einschränken**

   Informationen über Ereignisse im Betrieb der verwalteten Anwendungen werden vom Client-Gerät übertragen und in der Administrationsserver-Datenbank registriert. Um die Belastung auf den Administrationsserver zu reduzieren, sollten Sie die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, einschätzen und einschränken.

   Anleitung:

   - Verwaltungskonsole: Beschränkung der maximalen Anzahl der Ereignisse
   - Kaspersky Security Center Web Console: Beschränkung der maximalen Anzahl der Ereignisse

Ergebnisse

Nach Abschluss dieses Szenarios wird Ihr Netzwerk dank der Konfiguration von Kaspersky-Anwendungen, den Aufgaben und der vom Administrationsserver empfangenen Ereignissen geschützt sein.

- Die Kaspersky-Anwendungen werden entsprechend den Richtlinien und Richtlinienprofilen konfiguriert.
- Die Anwendungen werden über eine Reihe von Aufgaben verwaltet.
- Die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, ist eingestellt.

Wenn der Netzwerkschutz angepasst ist, können Sie mit der Konfiguration von regelmäßigen Updates für die Kaspersky-Datenbanken und -Programme fortfahren.

Weitere Informationen zum Konfigurieren von automatischen Reaktionen auf Bedrohungen, die durch Kaspersky Sandbox entdeckt wurden, finden Sie in der Online-Hilfe von Kaspersky Sandbox 2.0.

Geräteorientierte und benutzerorientierte Methode der Sicherheitsverwaltung

Sie können die Sicherheitseinstellungen unter Berücksichtigung der Gerätefunktionen oder der Benutzerrollen verwalten. Die erste Methode wird *geräteorientierte Sicherheitsverwaltung* genannt, die zweite *benutzerorientierte Sicherheitsverwaltung*. Um verschiedene Programmeinstellungen auf verschiedene Geräte anzuwenden, können Sie eine dieser Verwaltungsmethoden oder eine Kombination aus beiden Methoden verwenden. Zur Implementierung einer geräteorientierten Sicherheitsverwaltung können Sie die Werkzeuge nutzen, die von der Microsoft Management Console-basierten Verwaltungskonsole oder von der Kaspersky Security Center Web Console bereitgestellt werden. Die benutzerorientierte Sicherheitsverwaltung kann nur mithilfe der Kaspersky Security Center Web Console erfolgen.

Mit der gerätezentrierten Sicherheitsverwaltung können Sie je nach gerätespezifischen Merkmalen unterschiedliche Einstellungen der Sicherheitsanwendung auf verwaltete Geräte anwenden. So können Sie beispielsweise Geräte, die in verschiedenen Administrationsgruppen zugeordnet sind, mit unterschiedlichen Einstellungen versehen. Sie können die Geräte auch anhand der Verwendung dieser Geräte in Active Directory oder deren Hardware-Spezifikationen unterscheiden.

Die benutzerorientierte Sicherheitsverwaltung ermöglicht es Ihnen, verschiedene Einstellungen der Sicherheitsanwendung auf verschiedene Benutzerrollen anzuwenden. Sie können mehrere Benutzerrollen anlegen, jedem Benutzer eine entsprechende Benutzerrolle zuweisen und verschiedene Anwendungseinstellungen für die Geräte definieren, die sich im Besitz von Benutzern mit unterschiedlichen Rollen befinden. So können Sie zum Beispiel den Geräten von Buchhaltern und den Geräten von Mitarbeitern der Personalabteilung unterschiedliche Anwendungseinstellungen zuweisen. Als Ergebnis erhält bei der benutzerorientierten Sicherheitsverwaltung jede Abteilung – die Buchhaltung und die Personalabteilung – eine eigene Konfiguration der Einstellungen für Kaspersky-Anwendungen. Die Konfiguration der Einstellungen legt fest, welche Anwendungseinstellungen von Benutzern angepasst werden können und welche zwangsweise übernommen und durch den Administrator gesperrt sind.

Bei der benutzerorientierten Sicherheitsverwaltung können Sie einzelnen Benutzern bestimmte Programmeinstellungen zuweisen. Das ist z. B. sinnvoll, wenn ein Mitarbeiter eine besondere Rolle im Unternehmen einnimmt oder wenn Sie Sicherheitsvorfälle überwachen möchten, die auf dem Gerät einer bestimmten Person auftreten. Unter Berücksichtigung der Rolle des Mitarbeiters im Unternehmen können Sie die Berechtigung dieser Person zur Änderung der Programmeinstellungen erweitern oder einschränken. So würden Sie z. B. die Berechtigungen eines Systemadministrators, der Client-Geräte im lokalen Büro verwaltet, erweitern.

Es ist auch eine Kombination der geräteorientierten und der benutzerorientierten Herangehensweise an die Sicherheitsverwaltung möglich. So können Sie zum Beispiel für jede Administrationsgruppe eine bestimmte Anwendungsrichtlinie anpassen und Richtlinienprofile für eine oder mehrere Benutzerrollen Ihres Unternehmens erstellen. In diesem Fall werden die Richtlinien und Richtlinienprofile in der folgenden Reihenfolge angewendet:

1. Es werden Richtlinien angewendet, die für geräteorientierte Sicherheitsverwaltung erstellt wurden.
2. Sie werden mittels Richtlinienprofilen gemäß den Prioritäten der Profile geändert.
3. Die Richtlinien werden von den Richtlinienprofilen geändert, die Benutzerrollen zugewiesen sind.

Richtlinien einrichten und verwalten: geräteorientierte Herangehensweise

Nach Abschluss dieses Szenarios werden die Anwendungen gemäß den von Ihnen festgelegten Richtlinien und Richtlinienprofilen auf allen verwalteten Geräten konfiguriert.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie den Kaspersky Security Center Administrationsserver und die Kaspersky Security Center Web Console (optional) installiert haben. Wenn Sie die Kaspersky Security Center Web Console installiert haben, werden Sie womöglich die benutzerorientierte Sicherheitsverwaltung als Alternative oder als zusätzliche Option zur geräteorientierten Herangehensweise in Betracht ziehen.

Schritte

Das Szenario der geräteorientierten Verwaltung der Kaspersky-Anwendungen umfasst die folgenden Schritte:

1. **Anwendungsrichtlinien anpassen**

   Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Anwendungen an, indem Sie für jede Anwendung eine Richtlinie erstellen. Diese Auswahl an Richtlinien wird an die Client-Geräte weitergegeben.

   Wenn Sie den Schutz Ihres Netzwerks im Schnellstartassistenten konfigurieren, erstellt Kaspersky Security Center eine Standardrichtlinie für die folgenden Programme:

   - Kaspersky Endpoint Security für Windows – für Windows-basierte Client-Geräte
   - Kaspersky Endpoint Security für Linux – für Linux-basierte Client-Geräte

   Wenn Sie den Konfigurationsvorgang mithilfe dieses Assistenten abgeschlossen haben, müssen Sie keine neue Richtlinie für dieses Programm erstellen. Fahren Sie mit der manuellen Konfiguration der Richtlinie für Kaspersky Endpoint Security fort.

   Wenn Sie eine hierarchische Struktur aus mehreren Administrationsservern und/oder Administrationsgruppen haben, erben die sekundären Administrationsserver und die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen und an den sekundären Administrationsserver erzwingen, um Änderungen an den durch die Richtlinie höherer Ebene festgelegten Einstellungen zu verhindern. Wenn Sie möchten, dass nur bestimmte Einstellungen zwangsweise vererbt werden, können Sie diese in der Richtlinie höherer Ebene sperren. Die übrigen, nicht gesperrten Einstellungen können in den Richtlinien niedriger Ebene geändert werden. Dank der erstellten Hierarchie aus Richtlinien können Sie die Geräte in den Administrationsgruppen optimal verwalten.

Anleitung:

- Verwaltungskonsole: Richtlinie erstellen
- Kaspersky Security Center Web Console: Richtlinie erstellen

2. **Richtlinienprofile erstellen (optional)**

   Wenn Sie möchten, dass Geräte innerhalb einer Administrationsgruppe verschiedene Richtlinieneinstellungen erhalten, erstellen Sie Richtlinienprofile für diese Geräte. Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von der "zugrundeliegenden" Richtlinie unterscheiden, die auf dem verwalteten Gerät aktiv ist.

   Die Verwendung von Bedingungen zur Aktivierung von Profilen erlaubt die Anwendung verschiedener Richtlinienprofile auf Geräte, die sich z. B. in einer bestimmten Einheit oder Sicherheitsgruppe des Active Directory befinden, eine bestimmte Hardware-Konfiguration besitzen oder mit besonderen Tags markiert sind. Verwenden Sie Tags, um Geräte anhand bestimmter Kriterien zu filtern. So können Sie z. B. das Tag *Windows* erstellen, es allen Geräten mit einem Windows-Betriebssystem zuweisen und dieses Tag dann als Bedingung zur Aktivierung eines Richtlinienprofils festlegen. Als Ergebnis werden alle Kaspersky-Anwendungen, die auf Windows-Geräten installiert sind, von ihrem eigenen Richtlinienprofil verwaltet.

   Anleitung:

   - Verwaltungskonsole:
     - Richtlinienprofil erstellen
     - Regeln für die Aktivierung des Richtlinienprofils erstellen
   - Kaspersky Security Center Web Console:
     - Richtlinienprofil erstellen
     - Regeln für die Aktivierung des Richtlinienprofils erstellen

3. **Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergeben**

   Standardmäßig wird der Administrationsserver alle 15 Minuten automatisch mit den verwalteten Geräten synchronisiert. Sie können die automatische Synchronisierung umgehen und die Synchronisierung auch manuell mit dem Befehl Synchronisierung erzwingen ausführen. Die Synchronisierung wird auch erzwungen, nachdem Sie eine Richtlinie oder ein Richtlinienprofil erstellt oder geändert haben. Während der Synchronisierung werden neue oder veränderte Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergegeben.

   Wenn Sie die Kaspersky Security Center Web Console verwenden, können Sie überprüfen, ob die Richtlinien und Richtlinienprofile an ein bestimmtes Gerät übertragen wurden. Kaspersky Security Center registriert das Datum und die Uhrzeit der Weitergabe in den Eigenschaften des Geräts.

   Anleitung:

   - Verwaltungskonsole: Erzwungene Synchronisierung
   - Kaspersky Security Center Web Console: Erzwungene Synchronisierung

Ergebnisse

Nach Abschluss des geräteorientierten Szenarios werden die Kaspersky-Anwendungen gemäß den festgelegten Einstellungen konfiguriert und mittels Richtlinienhierarchie weitergegeben.

Die konfigurierten Anwendungsrichtlinien und Richtlinienprofile werden automatisch auf neue Geräte angewendet, die zu den Administrationsgruppen hinzugefügt werden.

Richtlinien einrichten und verwalten: benutzerorientierte Herangehensweise

Dieser Abschnitt beschreibt das Szenario der benutzerorientierten Herangehensweise an die zentralisierte Konfiguration der Kaspersky-Anwendungen, die auf den verwalteten Geräten installiert sind. Nach Abschluss dieses Szenarios werden die Programme gemäß den von Ihnen festgelegten Richtlinien und Richtlinienprofilen auf allen verwalteten Geräten konfiguriert.

Dieses Szenario kann mit der Kaspersky Security Center Web Console ab Version 13 implementiert werden.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie den Kaspersky Security Center Administrationsserver und die Kaspersky Security Center Web Console erfolgreich installiert und das Hauptinstallationsszenario beendet haben. Sie sollten zusätzlich auch die geräteorientierte Sicherheitsverwaltung als Alternative oder als zusätzliche Option zur benutzerorientierten Herangehensweise in Betracht ziehen. Weitere Informationen über beiden Verwaltungsmethoden.

Prozess

Das Szenario der benutzerorientierten Verwaltung der Kaspersky-Anwendungen umfasst die folgenden Schritte:

1. **Programmrichtlinien anpassen**

   Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Anwendungen an, indem Sie für jede Anwendung eine Richtlinie erstellen. Diese Auswahl an Richtlinien wird an die Client-Geräte weitergegeben.

   Wenn Sie den Schutz Ihres Netzwerks im Schnellstartassistenten konfigurieren, erstellt Kaspersky Security Center eine Standardrichtlinie für Kaspersky Endpoint Security. Wenn Sie den Konfigurationsvorgang mithilfe dieses Assistenten abgeschlossen haben, müssen Sie keine neue Richtlinie für dieses Programm erstellen. Fahren Sie mit der manuellen Konfiguration der Richtlinie für Kaspersky Endpoint Security fort.

   Wenn Sie eine hierarchische Struktur aus mehreren Administrationsservern und/oder Administrationsgruppen haben, erben die sekundären Administrationsserver und die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen und an den sekundären Administrationsserver erzwingen, um Änderungen an den durch die Richtlinie höherer Ebene festgelegten Einstellungen zu verhindern. Wenn Sie möchten, dass nur bestimmte Einstellungen zwangsweise vererbt werden, können Sie diese in der Richtlinie höherer Ebene sperren. Die übrigen, nicht gesperrten Einstellungen können in den Richtlinien niedriger Ebene geändert werden. Dank der erstellten Hierarchie aus Richtlinien können Sie die Geräte in den Administrationsgruppen optimal verwalten.

   Anleitung: Richtlinie erstellen

2. **Gerätebenutzer angeben**

   Weisen Sie die verwalteten Geräte den entsprechenden Benutzern zu.

   Anleitung: Festlegen eines Benutzers als Gerätebesitzer

3. **Typische Benutzerrollen in Ihrem Unternehmen festlegen**

   Überlegen Sie, in welchen unterschiedlichen Bereichen die Mitarbeiter Ihres Unternehmens tätig sind. Teilen Sie alle Mitarbeiter nach ihren Rollen ein. Sie können sie z. B. nach Abteilungen, Berufen oder Positionen unterteilen. Anschließend müssen Sie für jede Gruppe eine Benutzerrolle erstellen. Bedenken Sie, dass jede Benutzerrolle ihr eigenes Richtlinienprofil mit rollenspezifischen Anwendungseinstellungen erhält.

4. **Benutzerrollen erstellen**

   Erstellen und konfigurieren Sie eine Benutzerrolle für jede der Mitarbeitergruppen, die Sie im vorherigen Schritt festgelegt haben, oder verwenden Sie vorkonfigurierte Benutzerrollen. Die Benutzerrollen enthalten eine Auswahl an Zugriffsrechten für Anwendungsfunktionen.

   Anleitung: Benutzerrolle erstellen

5. **Umfang jeder Benutzerrolle festlegen**

   Geben Sie für jede erstellte Benutzerrolle die Benutzer und/oder die Sicherheitsgruppen und Administrationsgruppen an. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

   Anleitung: Bearbeiten des Bereichs einer Benutzerrolle

6. **Richtlinienprofile erstellen**

   Erstellen Sie für jede Benutzerrolle in Ihrem Unternehmen ein Richtlinienprofil. Die Richtlinienprofile bestimmen, welche Einstellungen für die auf den Benutzergeräten installierten Anwendungen gelten, wobei die Rolle jedes Benutzers berücksichtigt wird.

   Anleitung: Richtlinienprofil erstellen

7. **Richtlinienprofile mit Benutzerrollen verbinden**

   Verbinden Sie die erstellten Richtlinienprofile mit den Benutzerrollen. Das Richtlinienprofil gilt dann für Benutzer mit der festgelegten Rolle. Die im Richtlinienprofil angepassten Einstellungen werden auf Kaspersky-Anwendungen angewendet, die auf den Benutzergeräten installiert sind.

   Anleitung: Verbinden von Richtlinienprofilen mit Rollen

8. **Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergeben**

   Standardmäßig wird der Administrationsserver alle 15 Minuten automatisch mit den verwalteten Geräten synchronisiert. Während der Synchronisierung werden neue oder veränderte Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergegeben. Sie können die automatische Synchronisierung umgehen und die Synchronisierung auch manuell mit dem Befehl Synchronisierung erzwingen ausführen. Sobald die Synchronisierung abgeschlossen ist, werden die Richtlinien und Richtlinienprofile an die installierten Kaspersky-Anwendungen weitergegeben und von ihnen übernommen.

   Sie können überprüfen, ob die Richtlinien und Richtlinienprofile an ein bestimmtes Gerät übertragen wurden. Kaspersky Security Center registriert das Datum und die Uhrzeit der Weitergabe in den Eigenschaften des Geräts.

   Anleitung: Erzwungene Synchronisierung

Ergebnisse

Nach Abschluss des benutzerorientierten Szenarios werden die Kaspersky-Anwendungen gemäß den festgelegten Einstellungen konfiguriert und mittels der Hierarchie von Richtlinien und Richtlinienprofilen weitergegeben.

Für einen neuen Benutzer muss ein neues Benutzerkonto erstellt werden. Anschließend müssen dem Benutzer eine der erstellten Benutzerrollen sowie Geräte zugewiesen werden. Die konfigurierten Anwendungsrichtlinien und Richtlinienprofile werden automatisch auf die Geräte dieses Benutzers angewendet.

Richtlinieneinstellungen des Administrationsagenten

Gehen Sie folgendermaßen vor, um die Richtlinieneinstellungen des Administrationsagenten anzupassen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf den Namen der Richtlinie für Administrationsagenten.

   Das Eigenschaftenfenster der Richtlinie des Administrationsagenten wird geöffnet.

Der Vergleichstabelle können Sie im Detail entnehmen, wie die folgenden Einstellungen je nach verwendetem Betriebssystemtyp angewendet werden.

Allgemein

Auf dieser Registerkarte können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Unter **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:
  - **Aktiv**

    Bei Auswahl dieser Option wird die Richtlinie aktiv.

    Diese Variante ist standardmäßig ausgewählt.
  - **Inaktiv**

    Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.
- In der Einstellungsgruppe **Einstellungen erben** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:
  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.
  - **Vererbung der Einstellungen an untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:
    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.
    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Auf dieser Registerkarte können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Ereignisse werden anhand der Ereigniskategorie in die folgenden Abschnitte auf der Registerkarte **Konfiguration von Ereignissen** aufgeteilt:

- **Funktionsfehler**
- **Warnung**
- **Information**

In jedem Abschnitt führt die Liste mit Ereignistypen die Ereignistypen und die Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen) auf. Nachdem Sie den Ereignistyps angeklickt haben, können Sie die Eigenschaften für die Protokollierung und die Benachrichtigung über die aus der Liste ausgewählten Ereignisse festgelegt werden. Standardmäßig werden die allgemeinen Benachrichtigungseinstellungen, die für den gesamten Administrationsserver festgelegt wurden, für alle Ereignistypen verwendet. Bestimmte Einstellungen können jedoch für die gewünschten Ereignistypen angepasst werden.

Sie können beispielsweise im Abschnitt **Warnung** den Ereignistyp **Ein Sicherheitsvorfall ist eingetreten** konfigurieren. Solche Ereignisse können beispielsweise eintreten, wenn der freie Speicherplatz eines Verteilungspunkts weniger als 2GB beträgt (es sind mindestens 4 GB erforderlich, um Anwendungen remote zu installieren und Updates herunterzuladen). Um das Ereignis **Ein Sicherheitsvorfall ist eingetreten** zu konfigurieren, klicken Sie es an und legen Sie fest, wo die aufgetretenen Ereignisse gespeichert werden sollen und wie über sie benachrichtigt werden soll.

Wenn der Administrationsagent einen Sicherheitsvorfall entdeckt hat, können Sie diesen Vorfall mithilfe der Einstellungen eines verwalteten Geräts verwalten.

Programmeinstellungen

Einstellungen

Im Abschnitt **Einstellungen** können Sie die Richtlinieneinstellungen des Administrationsagenten anpassen:

- **Dateien nur über Verteilungspunkte übertragen**

  Wenn diese Option aktiviert ist, beziehen die Administrationsagenten auf verwalteten Geräten die Updates ausschließlich von Verteilungspunkten.

  Wenn diese Option deaktiviert ist, beziehen die Administrationsagenten auf verwalteten Geräten die Updates von Verteilungspunkten oder vom Administrationsserver.

  Beachten Sie, dass die Sicherheitsanwendungen auf verwalteten Geräten die Updates aus der Quelle abrufen, die in der Update-Aufgabe für jede Sicherheitsanwendung festgelegt wurde. Wenn Sie die Option **Dateien nur über Verteilungspunkte übertragen** aktivieren, stellen Sie sicher, dass Kaspersky Security Center in den Update-Aufgaben als Update-Quelle festgelegt ist.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Ereigniswarteschlange (MB)**

  In diesem Feld können Sie den maximalen Speicherplatz eingeben, welchen die Ereigniswarteschlange auf dem Laufwerk einnehmen kann.

  Standardmäßig ist der Wert auf 2 MB eingestellt.

- **Dem Programm ist es erlaubt, auf dem Gerät erweiterte Daten über Richtlinien zu erfassen**

  Der Administrationsagent, der auf einem verwalteten Gerät installiert ist, überträgt Informationen über die angewendete Sicherheitsanwendungs-Richtlinie an die Sicherheitsanwendung (z. B. Kaspersky Endpoint Security für Windows). Die übertragenen Informationen können Sie auf der Benutzeroberfläche der Sicherheitsanwendung einsehen.

  Der Administrationsagent überträgt die folgenden Informationen:

  - Zeit, zu der die Richtlinie dem verwalteten Gerät zugestellt wurde.
  - Name der aktiven Richtlinie zum Zeitpunkt der Übertragung der Richtlinien an das verwaltete Gerät.
  - Name der Richtlinie für mobile Benutzer zum Zeitpunkt der Übertragung der Richtlinie an das verwaltete Gerät. (für den Administrationsagenten für Linux nicht verfügbar).
  - Name und vollständiger Pfad der Administrationsgruppe, zu der das verwaltete Gerät gehörte, als die Richtlinie an das verwaltete Gerät zugestellt wurde.
  - Liste der aktiven Richtlinienprofile mit ihren Namen und Prioritäten zum Zeitpunkt der Übertragung der Richtlinien an das verwaltete Gerät.

  Sie können diese Informationen verwenden, um sicherzustellen, dass für das Gerät die richtige Richtlinie verwendet wird, und um Probleme zu lösen. Diese Option ist standardmäßig deaktiviert.

- **Dienst des Administrationsagenten vor unberechtigter Deinstallation und Beendigung schützen sowie Änderung der Einstellungen verhindern**

  Wenn diese Option aktiviert ist, kann nach der Installation des Administrationsagenten auf einem verwalteten Gerät die Komponente nicht ohne die entsprechenden Berechtigungen entfernt oder neu konfiguriert werden. Der Dienst des Administrationsagenten kann nicht beendet werden. Diese Option hat keine Auswirkung auf Domänencontroller.

  Aktivieren Sie diese Option, um den Administrationsagenten auf Workstations zu schützen, die mit lokalen Administratorrechten betrieben werden.

  Diese Option ist standardmäßig deaktiviert.

- **Deinstallationskennwort verwenden**

  Wenn diese Option aktiviert ist, können Sie das Kennwort für das Tool "klmover" und für die Aufgabe zur Remote-Deinstallation des Administrationsagenten angeben. Klicken Sie dazu auf die Schaltfläche **Ändern**.

  Diese Option ist standardmäßig deaktiviert.

Datenverwaltung

Im Abschnitt **Datenverwaltung** können Sie die Objekttypen auswählen, deren Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen. Wenn das Ändern der in diesem Abschnitt angegebenen Einstellungen in der Richtlinie des Administrationsagenten unterbunden ist, können Sie diese Einstellungen nicht ändern.

- **Details zu installierten Programmen**

  Ist diese Option aktiviert, werden auf den Administrationsserver Informationen über die auf den Client-Geräten installierten Anwendungen übertragen.

  Diese Option ist standardmäßig aktiviert.

- **Informationen über Patches einbinden**

  Informationen über die auf den Client-Geräten installierten Patches werden an den Administrationsserver übertragen. Das Aktivieren dieser Option kann die Auslastung des Administrationsservers und des DBMS erhöhen und eine Zunahme des Datenbankvolumens verursachen.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

- **Informationen über Windows-Updates**

  Wenn diese Option aktiviert ist, werden auf den Administrationsserver Informationen über Microsoft Windows-Updates übertragen, die auf den Client-Geräten installiert werden sollen.

  Selbst wenn die Option deaktiviert ist, werden Aktualisierungen manchmal in den Geräteeigenschaften im Abschnitt **Verfügbare Updates** angezeigt. Dies kann beispielsweise vorkommen, wenn die Geräte der Organisation Schwachstellen aufweisen, die durch diese Updates behoben werden können.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

  Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Informationen über Schwachstellen in Programmen und entsprechende Updates**

  Wenn diese Option aktiviert ist, werden Informationen über Schwachstellen in Dritthersteller-Anwendungen (Microsoft-Software eingeschlossen), die auf verwalteten Geräten erkannt wurden, sowie Informationen über Software-Updates zum Beheben der Dritthersteller-Schwachstellen (Microsoft-Software ausgeschlossen) an den Administrationsserver gesendet.

  Das Aktivieren der Option (**Informationen zu Schwachstellen in Programmen und entsprechenden Updates**) erhöht die Netzwerkbelastung, den Speicherbedarf des Administrationsservers und den Ressourcenverbrauch des Administrationsagenten.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

  Um Updates für Software von Microsoft zu verwalten, verwenden Sie die Option **Informationen über Windows-Updates**.

- **Informationen über die Hardware-Inventur**

  Der auf einem Gerät installierte Administrationsagent sendet Informationen über die Geräte-Hardware an den Administrationsserver. Sie können die Hardware-Details in den Geräteeigenschaften anzeigen.

  Stellen Sie sicher, dass das Tool "lshw" auf den Linux-Geräten installiert ist, von denen Sie die Hardwaredetails abrufen möchten. Die von virtuellen Maschinen abgerufenen Hardwaredetails können je nach verwendetem Hypervisor unvollständig sein.

Software-Updates und Schwachstellen

Im Abschnitt **Software-Updates und Schwachstellen** können Sie die Suche und Verteilung von Windows-Updates anpassen sowie die Untersuchung von ausführbaren Dateien auf Schwachstellen aktivieren:

- **Administrationsserver als WSUS-Server verwenden**

  Wenn diese Option aktiviert ist, werden die Windows-Updates auf den Administrationsserver heruntergeladen. Die heruntergeladenen Updates werden vom Administrationsserver zentralisiert für die Windows Update-Dienste mithilfe der Administrationsagenten auf den Client-Geräten bereitgestellt.

  Ist die Option deaktiviert, wird der Administrationsserver für den Download von Windows-Updates nicht verwendet. In diesem Fall erhalten die Client-Geräte die Windows-Updates selbständig.

  Diese Option ist standardmäßig deaktiviert.

- Sie können die Windows-Updates einschränken, welche die Benutzer auf ihren Geräten mithilfe von Windows Updates manuell installieren können.

  > Wenn auf Windows 10-Geräten der Windows Update-Dienst bereits Updates für das Gerät gefunden hat, wird die neue Option, die Sie unter **Benutzern die Verwaltung von Windows-Updates erlauben** auswählen können, erst angewendet, wenn die gefundenen Updates installiert wurden.

  Wählen Sie ein Element in der Dropdown-Liste:

  - **Benutzern die Installation aller anwendbaren Windows-Updates erlauben**

    Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar sind.

    Wählen Sie diese Option aus, wenn Sie nicht in die Installation von Updates eingreifen möchten.

    > Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

  - **Benutzern nur die Installation von genehmigten Windows-Updates erlauben**

    Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar und die von Ihnen genehmigt sind.

    Beispielsweise können Sie zuerst die Installation von Updates in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb von Geräten nicht stören, und erst dann die Installation dieser genehmigten Updates auf Client-Geräten erlauben.

    > Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

  - **Benutzern die Installation von Windows-Updates nicht erlauben**

    Benutzer können Microsoft Windows-Updates nicht manuell auf Ihren Geräten installieren. Alle anwendbaren Updates werden so installiert, wie sie von Ihnen angepasst wurden.

Wählen Sie diese Variante aus, wenn Sie die Installation von Updates zentral verwalten möchten.

Beispielsweise können Sie den Update-Zeitplan so optimieren, dass das Netzwerk nicht überlastet wird. Sie können Updates nach Büroschluss planen, damit sie sich nicht auf die Produktivität der Benutzer auswirken.

- In der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** können Sie den Modus für die Suche nach Updates auswählen:

  - **Aktiv**

    Wenn diese Option aktiviert ist, initiiert der Administrationsserver mit Unterstützung des Administrationsagenten eine Anfrage vom Windows Update-Agent des Client-Geräts zur Update-Quelle: Windows Update Server oder WSUS. Der Administrationsagent überträgt die vom Windows Update-Agent abgerufenen Daten an den Administrationsserver.

    Die Option wird nur wirksam, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** der Aufgabe *Finden von Schwachstellen und erforderlichen Updates* ausgewählt ist.

    Diese Variante ist standardmäßig ausgewählt.

  - **Passiv**

    Bei Auswahl dieser Option überträgt der Administrationsagent regelmäßig Informationen über Updates, die bei der letzten Synchronisierung des Windows Update-Agent mit der Update-Quelle abgerufen wurden, vom Windows-Update-Agenten an den Administrationsserver. Wird die Synchronisierung des Windows Update-Agenten mit der Update-Quelle nicht ausgeführt, veralten die Daten über Updates auf dem Administrationsserver.

    Wählen Sie diese Option aus, wenn Sie Updates aus dem Speicher-Cache der Update-Quelle abrufen möchten.

  - **Deaktiviert**

    Bei Auswahl dieser Option fragt der Administrationsserver keine Informationen über Updates ab.

    Wählen Sie diese Option aus, wenn Sie beispielsweise zuerst die Updates auf Ihrem lokalen Gerät testen möchten.

- **Ausführbare Dateien bei deren Start auf Schwachstellen untersuchen**

  Bei aktiviertem Kontrollkästchen werden ausführbare Dateien bei deren Start auf Schwachstellen untersucht.

  Diese Option ist standardmäßig aktiviert.

Verwaltung des Neustarts

Im Abschnitt **Verwaltung des Neustarts** können Sie die Aktion festlegen, die ausgeführt werden soll, wenn zur korrekten Ausführung, Installation oder Deinstallation des Programms ein Neustart des Betriebssystems des verwalteten Geräts erforderlich ist.

- **Betriebssystem nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Betriebssystem bei Bedarf automatisch neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn für das Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Variante ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen nach (Min.)**

    Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer mit der festgelegten Häufigkeit auf, das Betriebssystem neu zu starten.

    Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neustart erzwingen nach (Min.)**

    Nach der Aufforderung des Benutzers erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

    Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  - **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

    Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

    Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

    Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

    Diese Option ist standardmäßig deaktiviert.

Windows Desktopfreigabe

Im Abschnitt **Windows Desktopfreigabe** können Sie das Audit der Administrator-Tätigkeiten auf einem Remote-Gerät mit freigegebenem Desktop aktivieren und konfigurieren.

- **Audit aktivieren**

  Wenn diese Option aktiviert ist, dann ist das Audit des Administrators auf dem Remote-Gerät aktiviert. Einträge über die Aktionen des Administrators auf dem Remote-Gerät werden wie folgt gespeichert:

  - Im Ereignisprotokoll auf dem Remote-Gerät
  - In einer Datei mit der Erweiterung syslog, die sich im Installationsordner des Administrationsagenten auf dem Remote-Gerät befindet
  - In der Ereignisdatenbank von Kaspersky Security Center

  Das Audit des Administrators ist unter folgenden Bedingungen verfügbar:

  - Die Lizenz für das Schwachstellen- und Patch-Management wird verwendet
  - Der Administrator verfügt über die Berechtigung zum Start der Desktopfreigabe auf dem Remote-Gerät

  Wenn diese Option deaktiviert ist, dann ist das Audit des Administrators auf dem Remote-Gerät deaktiviert.

  Diese Option ist standardmäßig deaktiviert.

- **Masken für die Dateien, die bei Lesezugriff überwacht werden sollen**

  Diese Liste enthält Dateimasken. Wenn das Audit aktiviert ist, verfolgt das Programm, welche Dateien der entsprechenden Masken vom Administrator gelesen werden, und speichert Informationen über das Lesen von Dateien. Die Liste ist verfügbar, wenn das Kontrollkästchen **Audit aktivieren** aktiviert ist. Die Dateimasken können geändert und neue Masken zur Liste hinzugefügt werden. Neue Dateimasken müssen in der Liste in einer neuen Zeile hinzugefügt werden.

  Standardmäßig sind die Dateimasken *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf angegeben.

- **Masken der Dateien, die auf Änderung überwacht werden sollen**

  Die Liste enthält die Dateimasken auf dem Remote-Gerät. Wenn das Audit aktiviert ist, verfolgt das Programm, welche Dateien der entsprechenden Masken vom Administrator geändert werden, und speichert Informationen über die Änderung der Dateien. Die Liste ist verfügbar, wenn das Kontrollkästchen **Audit aktivieren** aktiviert ist. Die Dateimasken können geändert und neue Masken zur Liste hinzugefügt werden. Neue Dateimasken müssen in der Liste in einer neuen Zeile hinzugefügt werden.

  Standardmäßig sind die Dateimasken *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf angegeben.

Verwaltung von Patches und Updates

Im Abschnitt **Verwaltung von Patches und Updates** können Sie das Abrufen und Verteilen der Updates sowie die Installation der Patches auf den verwalteten Geräten anpassen:

- **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**

  Ist diese Option aktiviert, so werden Kaspersky-Patches, die den Genehmigungsstatus *Nicht definiert* haben, sofort automatisch auf den verwalteten Geräten installiert, nachdem sie von den Update-Servern heruntergeladen wurden.

  Wenn die Option deaktiviert ist, werden die Patches von Kaspersky, die heruntergeladen und mit dem Status *Nicht festgestellt* markiert sind, erst installiert, wenn Sie ihren Status auf *Genehmigt* ändern.

Diese Option ist standardmäßig aktiviert.

- **Updates und Antiviren-Datenbanken im Voraus vom Administrationsserver herunterladen (empfohlen)**

  Wenn diese Option aktiviert ist, wird das autonome Modell für das Abrufen von Updates verwendet. Wenn der Administrationsserver Updates empfängt, benachrichtigt der Administrationsagent (auf Geräten, auf denen er installiert ist) von den Updates, die für verwaltete Apps erforderlich sind. Wenn der Administrationsagent Informationen über diese Updates erhalten, ladet er die erforderlichen Dateien vom Administrationsserver im Voraus herunter. Bei der ersten Verbindung zum Administrationsagenten wird ein Updatedownload vom Administrationsserver initiiert. Nachdem der Administrationsagent alle Updates auf das Client-Gerät heruntergeladen hat, stehen die Updates den Programmen auf dem Gerät zur Verfügung.

  Wenn ein verwaltetes Programm auf dem Client-Gerät versucht, auf den Administrationsagenten zuzugreifen, um Updates herunterzuladen, überprüft der Administrationsagent, ob er über alle erforderlichen Updates verfügt. Wurden die Updates nicht mehr als 25 Stunden vor der Anfrage des verwalteten Programms vom Administrationsserver abgerufen, stellt der Administrationsagent keine Verbindung zum Administrationsserver her, sondern stellt dem verwalteten Programm die Updates aus dem lokalen Cache bereit. Eine Verbindung mit dem Administrationsserver wird möglicherweise nicht hergestellt, wenn der Administrationsagent Updates für Programme auf Client-Geräten bereitgestellt, für die Updates jedoch keine Verbindung erforderlich ist.

  Wenn diese Option deaktiviert ist, wird das autonome Modell für das Abrufen von Updates nicht verwendet. Updates werden gemäß dem Zeitplan der Aufgaben zum Update-Download verteilt.

  Diese Option ist standardmäßig aktiviert.

Konnektivität

Der Abschnitt **Konnektivität** enthält drei Unterabschnitte:

- **Netzwerk**
- **Verbindungsprofile**
- **Verbindungszeitplan**

Im Unterabschnitt **Netzwerk** können Sie die Einstellungen für die Verbindung zum Administrationsserver anpassen, die Nutzung eines UDP-Ports aktivieren und die Nummer des UDP-Ports festlegen.

- In der Einstellungsgruppe **Mit dem Administrationsserver verbinden** können Sie die Verbindungseinstellungen für den Administrationsserver anpassen und das Synchronisierungsintervall der Client-Geräte mit dem Administrationsserver festlegen:

  - **Synchronisierungsintervall (Min.)**

    Der Administrationsagent synchronisiert das verwaltete Gerät mit dem Administrationsserver. Es wird empfohlen, das Synchronisierungsintervall (auch als Herzschlag bezeichnet) auf 15 Minuten pro 10.000 verwaltete Geräte einzurichten.

    Bei einem Synchronisierungsintervall kleiner als 15 Minuten, wird die Synchronisierung alle 15 Minuten durchgeführt. Bei einem Synchronisierungsintervall größer gleich 15 Minuten, wird die Synchronisierung entsprechend des angegebenen Synchronisierungsintervalls durchgeführt.

- **Netzwerkverkehr komprimieren**

  Aktivieren Sie diese Option, um die Geschwindigkeit der Datenübertragung durch den Administrationsagenten zu steigern, das Datenvolumen zu komprimieren und die Belastung für den Administrationsserver zu reduzieren.

  > Die CPU-Auslastung des Client-Computers kann ansteigen.

  Dieses Kontrollkästchen ist standardmäßig aktiviert.

- **Ports des Administrationsagenten in der Windows-Firewall öffnen**

  Wenn diese Option aktiviert ist, werden die Ports, die für die Arbeit des Administrationsagenten und Administrationsservers erforderlich sind, zur Ausschlussliste der Microsoft Windows Firewall hinzugefügt.

  Diese Option ist standardmäßig aktiviert.

- **SSL-Verbindung verwenden**

  Wenn diese Option aktiviert ist, erfolgt die Verbindung zum Administrationsserver über einen gesicherten Port mit SSL-Protokoll.

  Diese Option ist standardmäßig aktiviert.

- **Verbindungs-Gateway auf einem Verteilungspunkt (falls vorhanden) mit den Standard-Verbindungseinstellungen verwenden**

  Wenn die Option aktiviert ist, wird das Verbindungs-Gateway auf dem Verteilungspunkt mit den Einstellungen verwendet, die in den Administrationsgruppeneigenschaften festgelegt sind.

  Diese Option ist standardmäßig aktiviert.

- **UDP-Port verwenden**

  Wenn es erforderlich ist, dass sich der Administrationsagent über einen UDP-Port mit dem Administrationsserver verbindet, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine **UDP-Portnummer** an. Diese Option ist standardmäßig aktiviert. Der standardmäßige UDP-Port für die Verbindung zum Administrationsserver ist 15000.

- **UDP-Port**

  Im Eingabefeld können Sie die Nummer des UDP-Ports eingeben. Standardmäßig wird Portnummer 15000 verwendet.

  Für die Eingabe wird das Dezimalformat verwendet.

  Wenn auf einem Client-Gerät das Betriebssystem Microsoft Windows XP Service Pack 2 installiert ist, blockiert die integrierte Firewall den UDP-Port mit der Nummer 15000. In diesem Fall muss der Port manuell geöffnet werden.

- **Verteilungspunkt verwenden, um eine Verbindung mit dem Administrationsserver zu erzwingen**

  Wählen Sie diese Option, wenn Sie im Fenster mit den Einstellungen des Verteilungspunktes die Option **Diesen Verteilungspunkt als Push-Server verwenden** ausgewählt haben. Andernfalls wird der Verteilungspunkt nicht als Push-Server fungieren.

Im Unterabschnitt **Verbindungsprofile** können Sie die Einstellungen des Netzwerkstandortes festlegen und den Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist:

- **Einstellungen des Netzwerkstandorts**

  Die Einstellungen des Netzwerkspeicherorts bestimmen die Merkmale des Netzwerks, mit dem das Client-Gerät verbunden ist, und legen die Regeln für den Wechsel des Administrationsagenten von einem Administrationsserver-Verbindungsprofil zu einem anderen fest (im Falle sich ändernder Merkmale des Netzwerks).

- **Verbindungsprofile des Administrationsservers**

  In diesem Abschnitt können Sie ein Profil für die Verbindung des Administrationsagenten mit dem Administrationsserver anzeigen und hinzufügen. In diesem Abschnitt können ferner die Umschaltregeln des Administrationsagenten auf andere Administrationsserver im Fall des Auftretens folgender Ereignisse festgelegt werden:

  - Verbindung des Client-Geräts mit einem anderen lokalen Netzwerk.
  - Trennung der Verbindung des Geräts vom lokalen Unternehmensnetzwerk.
  - Änderung der Verbindungs-Gateway-Adresse oder der Adresse des DNS-Servers.

  > Verbindungsprofile werden nur für Geräte mir Windows oder macOS unterstützt.

- **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**

  Wenn diese Option aktiviert ist, und eine Verbindung über dieses Profil besteht, verwenden Programme, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte im Modus für mobile Benutzer sowie Richtlinien für mobile Benutzer. Wurde für die Anwendung keine Richtlinie für mobile Benutzer definiert, verwendet die Anwendung die aktive Richtlinie.

  Wenn diese Option deaktiviert ist, wenden die Anwendungen die aktiven Richtlinien an.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Verbindungszeitplan** können Sie Zeitintervalle festlegen, in denen der Administrationsagent Daten auf den Administrationsserver übertragen soll:

- **Verbindung bei Bedarf herstellen**

  Bei dieser Variante wird eine Verbindung dann hergestellt, wenn Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen.

  Diese Variante ist standardmäßig ausgewählt.

- **Verbindung in den angegebenen Zeiträumen herstellen**

  Bei dieser Variante wird eine Verbindung des Administrationsagenten mit dem Administrationsserver in den vorgegebenen Zeiträumen hergestellt. Sie können mehrere Zeiträume für die Verbindung hinzufügen.

Netzwerkabfrage durch Verteilungspunkte

Im Abschnitt **Netzwerkabfrage durch Verteilungspunkte** können Sie die automatische Abfrage des Netzwerks anpassen. Sie können die folgenden Optionen verwenden, um die Abfrage zu aktivieren und ihre Häufigkeit festzulegen:

- **Windows-Netzwerk**

  Wenn diese Option aktiviert ist, fragt der Administrationsserver das Netzwerk automatisch gemäß dem Zeitplan ab, den Sie über die Links **Zeitplan für schnelle Abfrage festlegen** und **Zeitplan für vollständige Abfrage festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver das Netzwerk mit jenem Intervall ab, das im Feld **Intervall für Netzwerkabfragen (Min.)** angegeben ist.

  Das Intervall der Gerätesuche kann für Versionen des Administrationsagenten bis Version 10.2 in den Feldern **Intervall für Abfrage von Windows-Domänen (Min.)** (für schnelle Abfragen eines Windows-Netzwerks) und **Intervall für Netzwerkabfragen (Min.)** (für vollständige Abfragen eines Windows-Netzwerks) angepasst werden.

  Diese Option ist standardmäßig deaktiviert.

- **Zeroconf**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt das Netzwerk mit IPv6-Geräten unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) automatisch ab. In diesem Fall werden aktivierte IP-Bereichsabfragen ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt.

  Um Zeroconf verwenden zu können, müssen die folgenden Bedingungen erfüllt sein:

  - Der Verteilungspunkt muss unter Linux laufen.
  - Sie müssen auf dem Verteilungspunkt das Tool "avahi-browse" installieren.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt Netzwerke mit IPv6-Geräten nicht ab.

  Diese Option ist standardmäßig deaktiviert.

- **IP-Bereiche**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt die IP-Bereiche automatisch gemäß dem Zeitplan ab, den Sie über die Schaltfläche **Abfragezeitplan festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt keine IP-Bereiche ab.

  Das Intervall der Abfrage des IP-Bereichs kann für Versionen des Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Abschnitt ist verfügbar, wenn die Option aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

- **Domänencontroller**

  Wenn diese Option aktiviert ist, führt der Verteilungspunkt automatisch eine Abfrage des Active Directory gemäß dem Zeitplan durch, den Sie über den Link **Abfragezeitplan festlegen** eingestellt haben.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver das Active Directory nicht ab.

  Das Intervall der Abfrage des Active Directory kann für Versionen des Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Feld ist verfügbar, wenn diese Option aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt die Domänencontroller automatisch gemäß dem Zeitplan ab, den Sie über die Schaltfläche **Abfragezeitplan festlegen** eingerichtet haben.

Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt keine Domänencontroller ab.

Das Intervall für die Abfrage des Domänencontrollers kann für Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Feld ist verfügbar, wenn diese Option aktiviert ist.

Diese Option ist standardmäßig deaktiviert.

Netzwerk-Einstellungen für Verteilungspunkte

Wenn Ihre Verteilungspunkte für die Verbindung mit dem Internet einen Proxyserver verwenden, können Sie im Abschnitt **Netzwerk-Einstellungen für Verteilungspunkte** die folgenden Einstellungen festlegen:

- **Proxyserver verwenden**
- **Adresse**
- **Port**
- **Proxyserver für lokale Adressen umgehen**

  Wenn die Option aktiviert ist, wird bei der Verbindung mit den Geräten im lokalen Netzwerk kein Proxyserver verwendet.

  Diese Option ist standardmäßig deaktiviert.

- **Authentifizierung am Proxyserver**

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Benutzername**
- **Kennwort**

KSN Proxy (Verteilungspunkte)

Im Abschnitt **KSN Proxy (Verteilungspunkte)** können Sie die Anwendung anpassen, um den Verteilungspunkt zum Weiterleiten von Anfragen des Kaspersky Security Network (KSN) von den verwalteten Geräten zu verwenden:

- **KSN Proxy auf dem Verteilungspunkt aktivieren**

  Der KSN-Proxy-Service wird auf dem Gerät ausgeführt, das als Verteilungspunkt verwendet wird. Verwenden Sie diese Funktion, um Datenverkehr im Netzwerk neu zu verteilen und zu optimieren.

  Der Verteilungspunkt sendet die KSN-Statistik, die in der Erklärung zu Kaspersky Security Network aufgeführt sind, an Kaspersky.

  Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn im Fenster mit den Eigenschaften des Administrationsservers die Optionen **Administrationsserver als Proxyserver verwenden** und **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** aktiviert sind.

  Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

- **KSN-Anfragen an den Administrationsserver weiterleiten**

  Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an den Administrationsserver weiter.

  Diese Option ist standardmäßig aktiviert.

- **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**

  Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an die KSN Cloud oder an KPSN weiter. KSN-Anfragen, die der Verteilungspunkt selbst generiert, werden ebenso direkt an KSN Cloud oder KPSN gesendet.

  Verteilungspunkte, auf denen der Administrationsagent bis einschließlich Version 11 installiert ist, können nicht direkt auf KPSN zugreifen. Um die Verteilungspunkte so anzupassen, dass KSN-Anfragen an KPSN gesendet werden, aktivieren Sie für jeden Verteilungspunkt die Option **KSN-Anfragen an den Administrationsserver weiterleiten**.

  Verteilungspunkte, auf denen der Administrationsagent ab Version 12 installiert ist, können direkt auf KPSN zugreifen.

- **Port**

  Die Nummer des TCP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Standardmäßig wird Portnummer 13111 verwendet.

- **UDP-Port**

  Wenn es erforderlich ist, dass sich der Administrationsagent über einen UDP-Port mit dem Administrationsserver verbindet, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine **UDP-Portnummer** an. Diese Option ist standardmäßig aktiviert. Der standardmäßige UDP-Port für die Verbindung zum Administrationsserver ist 15000.

Updates (Verteilungspunkte)

Sie können die Funktion zum Download von diff-Dateien im Abschnitt **Updates (Verteilungspunkte)** aktivieren, damit die Verteilungspunkte die Updates in Form von diff-Dateien von den Kaspersky-Update-Servern erhalten.

Verwaltung lokaler Benutzerkonten (nur Linux)

Der Abschnitt **Verwaltung lokaler Benutzerkonten (nur Linux)** enthält drei Unterabschnitte:

- **Verwaltung von Benutzerzertifikaten**
- **Anwendbare lokale Administrationsgruppen hinzufügen oder bearbeiten**
- **Referenzdatei hochladen, um die sudoers-Datei auf dem Benutzergerät vor Änderungen zu schützen**

Im Unterabschnitt **Verwaltung von Benutzerzertifikaten** können Sie angeben, welche Stammzertifikate installiert werden sollen. Diese Zertifikate können beispielsweise verwendet werden, um die Authentizität von Websites oder Webservern zu überprüfen.

- **Root-Zertifikate installieren**

  Wenn diese Option aktiviert ist, werden die zur Tabelle hinzugefügten Zertifikate auf den angegebenen Geräten installiert.

  Wenn diese Option deaktiviert ist, werden auf den angegebenen Geräten keine Zertifikate installiert.

Diese Option ist standardmäßig deaktiviert.

- **Hinzufügen**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie ein Zertifikat hinzufügen können.

  Das Zertifikat muss kleiner als 10 MB sein.

  Kaspersky Security Center unterstützt Zertifikate mit folgenden Erweiterungen: cer, crt, cert, pem und key.

Im Unterabschnitt **Anwendbare lokale Administrationsgruppen hinzufügen oder bearbeiten** können Sie die Gruppen mit lokalen Administratoren verwalten. Diese Gruppen werden beispielsweise verwendet, wenn lokale Administratorrechte entzogen werden. Sie können die Liste der privilegierten Benutzerkonten auch mithilfe des **Bericht über privilegierte Gerätenutzer (nur Linux)** überprüfen.

- **Hinzufügen**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie eine Gruppe mit lokalen Administratoren hinzufügen können.

- **Bearbeiten**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie die Gruppe mit lokalen Administratoren bearbeiten können.

  Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Gruppe mit lokalen Administratoren aktiviert ist.

- **Löschen**

  Mit dieser Schaltfläche wird die ausgewählte Gruppe mit lokalen Administratoren aus der Tabelle gelöscht.

  Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Gruppe mit lokalen Administratoren aktiviert ist.

Im Unterabschnitt **Referenzdatei hochladen, um die sudoers-Datei auf dem Benutzergerät vor Änderungen zu schützen**, können Sie die Kontrolle der sudoers-Datei anpassen. Privilegierte Gruppen und Gerätebenutzer werden durch die sudoers-Datei auf dem Gerät definiert. Die sudoers-Datei befindet sich unter `/etc/sudoers`. Sie können eine sudoers-Referenzdatei hochladen, um die eigentliche sudoers-Datei vor Änderungen zu schützen. Dadurch werden unerwünschte Änderungen an der sudoers-Datei verhindert.

Eine ungültige sudoers-Referenzdatei kann zu Fehlfunktionen auf dem Gerät des Benutzers führen.

- **sudoers-Datei überwachen**

  Wenn diese Option aktiviert ist, wird die sudoers-Datei durch die aktuelle -sudoers-Referenzdatei ersetzt.

  Wenn diese Option deaktiviert ist, bleibt die sudoers-Datei unverändert.

  Diese Option ist standardmäßig deaktiviert.

- **sudoer-Referenzdatei**

  In diesem Feld wird der Name der hochgeladenen sudoers-Referenzdatei angezeigt.

- **Hochladen**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie sudoers-Referenzdatei können.

- **Aktuelle sudoers-Referenzdatei**

  Wenn Sie auf diese Schaltfläche klicken, wird der Inhalt der aktuellen sudoers-Datei angezeigt.

Revisionsverlauf

Auf dieser Registerkarte können Sie eine Liste mit Revisionen der Richtlinie anzeigen und bei Bedarf ein Rollback der Änderungen an der Richtlinie vornehmen.

Vergleich der Richtlinieneinstellungen des Administrationsagenten nach Betriebssystemen

Die folgende Tabelle zeigt, welche Richtlinieneinstellungen des Administrationsagenten Sie in der Verwaltungskonsole und der Kaspersky Security Center Web Console verwenden können, um den Administrationsagenten mit einem bestimmten Betriebssystem zu konfigurieren.

Richtlinieneinstellungen des Administrationsagenten: Vergleich nach Betriebssystemen

Richtlinienabschnitt	Windows	macOS	Linux
Allgemein	✓	✓	✓
Konfiguration von Ereignissen	✓	✓	✓
Einstellungen	✓	✓	✓ Es sind folgende Optionen verfügbar: • **Dateien nur über Verteilungspunkte übertragen** • **Maximale Größe der Ereigniswarteschlange (MB)** • **Dem Programm ist es erlaubt, auf dem Gerät erweiterte Daten über Richtlinien zu erfassen**
Datenverwaltung	✓	✓ Die Option **Informationen über das Hardware-Register** ist verfügbar.	✓ Es sind folgende Optionen verfügbar: • **Details zu installierten Programmen** • **Informationen über die Hardware-Inventur**
Software-Updates und Schwachstellen	✓	—	—
Verwaltung des Neustarts	✓	—	—
Windows Desktopfreigabe	✓	—	—
Verwaltung von Patches und Updates	✓	—	—
Konnektivität → Netzwerk	✓	✓	✓ Mit Ausnahme der Option **Ports des Administrationsagenten in der Windows-Firewall öffnen**.
Konnektivität → Verbindungsprofile	✓	✓	—
Konnektivität → Verbindungszeitplan	✓	✓	✓
Netzwerkabfrage durch Verteilungspunkte	✓ Es sind nur die Optionen **Windows-Netzwerk**, **IP-Bereiche** und **Domänencontroller** verfügbar.	—	✓ Es sind folgende Optionen verfügbar: • **Zeroconf** • **IP-Bereiche** • **Domänencontroller**

Richtlinienabschnitt	Windows	macOS	Linux
Netzwerk-Einstellungen für Verteilungspunkte	✓	✓	✓
KSN Proxy (Verteilungspunkte)	✓	—	✓
Updates (Verteilungspunkte)	✓	—	✓
Revisionsverlauf	✓	✓	✓

Modus für geringem Ressourcenverbrauch des Administrationsagenten aktivieren und deaktivieren

Im ressourcenschonenden Modus können Sie auf dem Client-Gerät die Auslastung des Arbeitsspeichers durch den installierten Administrationsagenten einschränken. Der ressourcenschonende Modus ist standardmäßig deaktiviert.

Im ressourcenschonenden Modus werden die folgenden Funktionen nicht ausgeführt:

- Der Administrationsagent kann nicht als Verteilungspunkt zugewiesen werden (weder manuell noch automatisch).
- Der Administrationsagent protokolliert keine Informationen über den Status des Administrationsagenten in einer separaten Textdatei.
- Der Administrationsagent unterstützt das Offline-Modell für Update-Downloads nicht.
- Die folgenden Komponenten und Prozesse sind deaktiviert:
  - Abrufen von Informationen über Drittanbieter-Updates und Schwachstellen.
  - Ausführen des KSN Proxy auf dem Verteilungspunkt.
  - Hochladen von Updates in die Datenverwaltung des Verteilungspunkts.
  - Umgehen der DNS-Server-Sperre.
  - Abrufen von Informationen über freien Speicherplatz.

Wenn der ressourcenschonende Modus deaktiviert wird, werden die Komponenten und Prozesse wieder ausgeführt.

So aktivieren Sie den ressourcenschonenden Modus:

1. Führen Sie in der Befehlszeile den folgenden Befehl aus:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Starten Sie den Administrationsagent neu.

3. Um zu überprüfen, ob der Modus für geringen Ressourcenverbrauch aktiviert ist, öffnen Sie in Windows die **Ereignisanzeige** und wählen Sie anschließend **Anwendungs- und Dienstprotokolle → Kaspersky-Ereignisprotokoll** aus.

   Stellen Sie sicher, dass das Protokoll Ereignisse wie **Kaspersky Security Center Administrationsagent wird im Modus mit geringem Ressourcenverbrauch ausgeführt** enthält.

Der ressourcenschonende Modus ist aktiviert.

So deaktivieren Sie den ressourcenschonenden Modus:

1. Führen Sie in der Befehlszeile den folgenden Befehl aus:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Starten Sie den Administrationsagent neu.

3. Um zu überprüfen, ob der Modus für geringen Ressourcenverbrauch deaktiviert ist, öffnen Sie in Windows die **Ereignisanzeige** und wählen Sie anschließend **Anwendungs- und Dienstprotokolle → Kaspersky-Ereignisprotokoll** aus.

   Stellen Sie sicher, dass das Protokoll keine Ereignisse wie **Kaspersky Security Center Administrationsagent wird im Modus mit geringem Ressourcenverbrauch ausgeführt** enthält.

Der ressourcenschonende Modus ist deaktiviert.

Sie können den Modus für geringem Ressourcenverbrauch auch remote aktivieren, indem Sie die Aufgabe *Remote-Ausführung von Skripten* verwenden.

Konfigurieren der Schutzeinstellungen für verwaltete Anwendungen

Zum Konfigurieren der Schutzeinstellungen für verwaltete Kaspersky-Anwendungen können Sie Richtlinien verwenden.

Weitere Informationen zum Konfigurieren von Richtlinien für Kaspersky Endpoint Security finden Sie in den entsprechenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux
- Hilfe zu Kaspersky Endpoint Security for Mac

Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren

Der optimale und empfohlene Zeitplan für Kaspersky Endpoint Security ist **Nach dem Download von Updates in die Datenverwaltung**, wenn das Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert ist.

Programme oder Software-Updates remote löschen

Um Programme oder Software-Updates von ausgewählten Geräten remote zu entfernen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Remote-Deinstallation eines Programms**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen.

   Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.
6. Wählen Sie aus, welche Art von Software Sie entfernen wollen, und wählen Sie anschließend bestimmte Programme, Updates oder Patches aus, die Sie entfernen wollen:

   - **Verwaltetes Programm deinstallieren**

     Eine Liste mit Kaspersky-Anwendungen wird angezeigt. Wählen Sie die Anwendung aus, die Sie entfernen möchten.

   - **Inkompatibles Anwendung deinstallieren**

     Eine Liste mit Anwendungen, die nicht kompatibel zu Kaspersky-Sicherheitsanwendungen oder zu Kaspersky Security Center sind, wird angezeigt. Aktivieren Sie die Kontrollkästchen neben den Anwendungen, die Sie entfernen möchten.

   - **Programm aus der Programm-Registry deinstallieren**

     Standardmäßig übertragen Administrationsagenten die Information über Anwendungen, die auf verwalteten Geräten installiert sind, an den Administrationsserver. Die Liste der installierten Anwendungen wird in der Programm-Registry gespeichert.

     So wählen Sie eine Anwendung aus der Programm-Registry aus:

     a. Klicken Sie auf das Feld **Zu deinstallierendes Programm** und wählen Sie anschließend die Anwendung aus, die Sie entfernen wollen.

     > Wenn Sie beim Ausführen der Aufgabe das Programm "Kaspersky Security Center Administrationsagent" auswählen, zeigt der Status *Erfolgreich abgeschlossen* an, dass der Deinstallationsvorgang gestartet wurde. Nach dem Löschen des Kaspersky Security Center Administrationsagenten ändert sich der Status nicht. Wenn die Aufgabe fehlschlägt, ändert sich der Status in *Fehlgeschlagen*.

b. Geben Sie die folgenden Optionen für die Deinstallation an:

- **Deinstallationsmodus**

  Wählen Sie aus, wie Sie die Anwendung entfernen möchten:

  - **Deinstallationsbefehl automatisch definieren**

    Wenn die Anwendung einen Deinstallationsbefehl besitzt, welcher durch den Hersteller der Anwendung vorgegeben wurde, nutzt Kaspersky Security Center diesen Befehl. Es wird empfohlen, diese Option auszuwählen.

  - **Deinstallationsbefehl angeben**

    Wählen Sie diese Option aus, wenn Sie einen eigenen Befehl für die Deinstallation der Anwendung angeben möchten.

    > Es wird empfohlen, das Entfernen der Anwendung zunächst unter Verwendung der Option **Deinstallationsbefehl automatisch definieren** auszuprobieren. Sollte die Deinstallation mit dem automatisch definierten Befehl fehlschlagen, verwenden Sie einen eigenen Befehl.

    Geben Sie einen Installationsbefehl in das Feld ein und geben Sie danach die folgende Option an:

    Diesen Deinstallationsbefehl nur dann verwenden, wenn der Standardbefehl nicht automatisch entdeckt wurde

    Kaspersky Security Center prüft, ob die ausgewählte Anwendung einen vom Hersteller der Anwendung vorgegeben Deinstallationsbefehl besitzt. Wenn so ein Befehl existiert, verwendet Kaspersky Security Center diesen anstelle des Befehls der in dem Feld **Deinstallationsbefehl des Programms** angegeben wurde.

    Es wird empfohlen, diese Option zu aktivieren.

- **Nach einer erfolgreichen Deinstallation einen Neustart durchführen**

  Wenn der Vorgang nach einer erfolgreichen Deinstallation einen Neustart des Betriebssystems auf dem verwalteten Gerät benötigt, wird das Betriebssystem automatisch neu gestartet.

- **Bestimmtes Programm-Update, einen Patch oder Dritthersteller-Programm deinstallieren**

  Es wird eine Liste mit Updates, Patches und Drittanbieter-Programmen angezeigt. Wählen Sie das Objekt aus, das Sie entfernen möchten.

  Die angezeigte Liste ist eine allgemeine Liste mit Anwendungen und Updates, die nicht den tatsächlich installierten Anwendungen und Updates auf den verwalteten Geräten entspricht. Es wird empfohlen, vor der Auswahl eines Objekts zu überprüfen, ob die Anwendung oder das Update tatsächlich auf dem im Aufgabenbereich festgelegten Geräten installiert ist. Sie können sich die Liste mit Geräten, auf denen die Anwendung oder das Update installiert ist, über das Eigenschaftenfenster anzeigen lassen.

  So zeigen Sie die Liste der Geräte an:

  a. Klicken Sie auf den Namen der Anwendung oder des Updates.

  Daraufhin wird das Eigenschaftenfenster geöffnet.

  b. Öffnen Sie den Abschnitt **Geräte**.

  Sie können sich die Liste mit installierten Anwendungen und Updates auch im Eigenschaftenfenster des Geräts ansehen.

7. Geben Sie an, auf welche Weise die Client-Geräte das Deinstallations-Hilfsprogramm herunterladen sollen:

- **Unter Nutzung des Administrationsagenten**

  Die Dateien werden den Client-Geräten mithilfe des Administrationsagenten, der auf den Geräten installiert ist, ausgeliefert.

  Wenn diese Option deaktiviert ist, werden die Dateien mithilfe der Tools von Microsoft Windows ausgeliefert.

  Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

- **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**

  Die Dateien werden mit den Betriebssystem-Tools des Administrationsservers an die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

- **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**

  Die Dateien werden mit Tools des Betriebssystems über Verteilungspunkte an die Client-Geräte ausgeliefert. Diese Option kann aktiviert werden, wenn sich mindestens ein Verteilungspunkt im Netzwerk befindet.

  Ist die Option **Unter Nutzung des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Tools des Betriebssystems zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

- **Maximale Anzahl gleichzeitiger Downloads**

  Die erlaubte Höchstzahl an Client-Geräten, an die der Administrationsserver simultan Dateien ausliefern kann. Je höher die Nummer, umso schneller werden die Anwendungen deinstalliert, aber umso höher ist auch die Auslastung des Administrationsservers.

- **Maximale Anzahl der Deinstallationsversuche**

  Wenn während der Ausführung der Aufgabe *Remote-Deinstallation eines Programms* für Kaspersky Security Center die Anzahl an Deinstallationsversuchen einer Anwendung auf einem verwalteten Gerät nicht innerhalb der Anzahl an Versuchen, die im Parameter angegeben wurde, erfolgreich ist, stoppt Kaspersky Security Center das Ausliefern des Deinstallationstools auf diesem verwalteten Gerät und startet die Installationsaufgabe auf dem Gerät nicht mehr.

  Der Parameter **Maximale Anzahl der Deinstallationsversuche** ermöglicht es Ihnen, die Ressourcen eines verwalteten Geräts zu sparen und den Datenverkehr zu reduzieren (Deinstallation, MSI-Datei ausführen und Fehlermeldungen).

  Wiederkehrende Versuche zum Aufgabestart können auf ein Problem auf dem Gerät hinweisen, das die Deinstallation verhindert. Der Administrator sollte das Problem innerhalb der angegebenen Anzahl an Deinstallationsversuchen lösen und die Aufgabe anschließend neu starten (manuell oder mittels Zeitplan).

  Wenn die Deinstallation nicht abgeschlossen werden kann, ist das Problem unter Umständen nicht lösbar und jeder weitere Aufgabenstart wäre ein unnützer Verbrauch von Ressourcen und Datenverkehr.

  Beim Erstellen der Aufgabe wird der Zähler für Versuche auf `0` gesetzt. Jede Ausführung des Installationsprogramms, die einen Fehler zurückgibt, erhöht den Zählerstand.

  Wenn die im Parameter angegebene Anzahl an Versuchen überschritten wurde und das Gerät für die Deinstallation der Anwendung bereit ist, können Sie den Wert **Maximale Anzahl der Deinstallationsversuche** erhöhen und die Deinstallations-Aufgabe starten. Alternativ können Sie eine neue Aufgabe des Typs *Remote-Deinstallation eines Programms* erstellen.

- **Typ des Betriebssystems vor dem Download prüfen**

  Bevor die Dateien auf die Client-Geräte übertragen werden, prüft Kaspersky Security Center, ob die Einstellungen des Installationstools auf dem Betriebssystem des Client-Geräts anwendbar sind. Wenn die Einstellungen nicht anwendbar sind, überträgt Kaspersky Security Center die Dateien nicht und wird nicht versuchen, die Anwendung zu installieren. So können Sie beispielsweise eine Anwendung auf den Geräten einer Administrationsgruppe, die mehrere Geräte mit unterschiedlichen Betriebssystemen enthält, installieren, indem Sie die Aufgabe zur Installation der Administrationsgruppe zuweisen und anschließend die Option zum Überspringen von Geräten mit davon abweichenden Betriebssystemen aktivieren.

  Wenn Sie den Administrationsagenten per Remote-Installation auf nicht zugeordneten Geräten installieren, bestimmt Kaspersky Security Center oder ein Verteilungspunkt das Betriebssystem des Geräts automatisch, unabhängig davon, welchen Wert die Einstellung **Typ des Betriebssystems vor dem Download prüfen** hat.

- **Deinstallationskennwort verwenden**

  Dieser Parameter wird angezeigt, wenn Sie im vorherigen Schritt die Option **Verwaltetes Programm deinstallieren** ausgewählt und anschließend im Feld **Zu deinstallierendes Programm** das Programm "Kaspersky Security Center Administrationsagent" angegeben haben.

  Wenn Sie zuvor das Kennwort für die Remote-Deinstallation des Administrationsagenten in den Richtlinieneinstellungen des Administrationsagenten festgelegt haben, aktivieren Sie das Kontrollkästchen **Deinstallationskennwort verwenden** und geben Sie das Deinstallationskennwort in das Feld **Kennwort** ein. Wenn Sie kein Kennwort für die Remote-Deinstallation des Administrationsagenten festgelegt haben, aktivieren Sie das Kontrollkästchen nicht.

8. Geben Sie die Einstellungen für den Neustart des Betriebssystems an:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

   - **Gerät neu starten**

     Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

   - **Benutzer fragen**

     Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

     Diese Option ist standardmäßig ausgewählt.

   - **Aufforderung regelmäßig wiederholen nach (Min.)**

     Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

     Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

9. Bei Bedarf können Sie Benutzerkonten hinzufügen, die für den Start der Aufgabe zur Remote-Deinstallation verwendet werden sollen:

   - **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

     Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm der Anwendung gestartet werden soll. Die Aufgabe wird unter dem Konto gestartet, unter dem der Dienst des Administrationsservers läuft.

     Wenn der Administrationsagent nicht auf den Client-Geräten installiert ist, steht diese Option nicht zur Verfügung.

   - **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**

     Wählen Sie diese Option, wenn auf den Geräten, denen Sie die Aufgabe zur *Remote-Deinstallation* zuweisen, der Administrationsagent nicht installiert ist. In diesem Fall können Sie ein Benutzerkonto oder ein SSH-Zertifikat angeben, um die Anwendung zu deinstallieren.

     - **Lokales Benutzerkonto**. Wenn Sie diese Variante auswählen, können Sie das Benutzerkonto angeben, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Benutzerkonto** aus, und geben Sie anschließend die Anmeldeinformationen des Benutzerkontos an.

       Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Benutzerkonto existiert, dass über die erforderlichen Rechte auf allen Geräten verfügt, für welche die Aufgabe bestimmt wurde. In diesem Fall werden für den Start der Aufgabe alle hinzugefügten Konten nacheinander von oben nach unten angewandt.

     - **SSH-Zertifikat**. Wenn Sie eine Anwendung von einem Linux-basierten Client-Gerät deinstallieren möchten, können Sie anstelle eines Benutzerkontos ein SSH-Zertifikat angeben. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **SSH-Zertifikat** aus, und geben Sie anschließend den privaten und den öffentlichen Schlüssel des Zertifikats an.

Um einen privaten Schlüssel zu generieren, können Sie das Tool "ssh-keygen" verwenden. Beachten Sie, dass die Kaspersky Security Center das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" den Parameter "-m PEM" hinzu.

Beispielsweise:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<Benutzer-E-Mail>"
```

10. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

11. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

12. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

13. Geben Sie im Fenster mit den Aufgabeneigenschaften die allgemeinen Aufgabeneinstellungen an.

14. Klicken Sie auf die Schaltfläche **Speichern**.

15. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Deinstallation wird die gewählte Anwendung von den ausgewählten Geräten entfernt.

Probleme bei der Remote-Deinstallation

Es kann passieren, dass bei der Remote-Deinstallation einer Drittanbieter-Anwendung die folgende Warnung angezeigt wird: "Die Remote-Deinstallation wurde auf diesem Gerät mit Warnungen abgeschlossen: Die zu entfernende Anwendung ist nicht installiert." Dieses Problem tritt auf, wenn die zu deinstallierende Anwendung bereits deinstalliert wurde oder nur für einen einzelnen Benutzer installiert ist. Anwendungen, die für einen einzelnen Benutzer installiert sind (auch als "benutzerspezifische Anwendungen" bezeichnet), werden unsichtbar und können nicht per Remote-Deinstallation entfernt werden, wenn dieser Benutzer nicht angemeldet ist.

Dieses Verhalten unterscheidet sich von Anwendungen, die von mehreren Benutzern auf demselben Gerät verwendet werden (auch als "gerätespezifische Anwendungen" bezeichnet). Gerätespezifische Anwendungen sind für alle Benutzer des Geräts sichtbar und zugänglich.

Aus diesem Grund können benutzerspezifische Anwendungen nur dann deinstalliert werden, wenn der Benutzer angemeldet ist.

Informationsquellen zu installierten Anwendungen

Auf Windows-Geräten ruft der Administrationsagent Informationen über installierte Software aus den folgenden Registrierungsschlüsseln ab:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für alle Benutzer installiert sind.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  Enthält Informationen über Anwendungen, die für alle Benutzer installiert sind.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Enthält Informationen über Anwendungen, die für den aktuellen Benutzer installiert sind.
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Enthält Informationen über Anwendungen, die für bestimmte Benutzer installiert sind.

Aufgaben

In diesem Abschnitt werden Aufgaben beschrieben, die von Kaspersky Security Center verwendet werden.

Über Aufgaben

Kaspersky Security Center verwaltet die auf Geräten installierten Sicherheitsanwendungen von Kaspersky durch das Erstellen und Starten von *Aufgaben*. Die Aufgaben ermöglichen Installation, Start und Beenden von Programmen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Programm-Module sowie Ausführung anderer Aktionen mit den Programmen.

Aufgaben für eine bestimmte Anwendung können mithilfe von Kaspersky Security Center Web Console nur dann erstellt werden, wenn das Verwaltungs-Plug-in für diese Anwendung auf dem Server der Web Console von Kaspersky Security Center installiert ist.

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Zu den Aufgaben, die auf dem Administrationsserver ausgeführt werden, gehören:

- Berichte automatisch versenden
- Updates in die Datenverwaltung herunterladen
- Backup der Daten des Administrationsservers anlegen
- Datenbank bedienen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

- *Lokale Aufgaben* sind Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

  Lokale Aufgaben können nicht nur vom Administrator mithilfe der Verwaltungskonsole geändert werden, sondern auch vom Benutzer des Remote-Geräts (beispielsweise in der Benutzeroberfläche der Sicherheitsanwendung). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

- *Gruppenaufgaben* sind Aufgaben, die auf allen Geräten einer bestimmten Gruppe ausgeführt werden.

  Soweit in den Aufgabeneigenschaften nicht anders festgelegt, betrifft eine Gruppenaufgabe auch alle Untergruppen der ausgewählten Gruppe. Eine Gruppenaufgabe betrifft (optional) auch Geräte, die mit den sekundären und virtuellen Administrationsservern in der Gruppe und den Untergruppen verbunden sind.

- *Globale Aufgaben* sind Aufgaben, die auf einem Satz von Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Gruppe gehören.

Sie können für jede Anwendung eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt von Aufgaben verfolgen, und Aufgaben kopieren, exportieren, importieren und löschen.

Eine Aufgabe wird auf einem Gerät nur dann gestartet, wenn die Anwendung gestartet wurde, für die diese Aufgabe erstellt wurde.

Ausführungsergebnisse von Aufgaben werden im Betriebssystem-Ereignisprotokolle auf jedem Gerät, im Betriebssystem-Ereignisprotokoll des Administrationsservers und in der Administrationsserver-Datenbank gespeichert.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Über den Gültigkeitsbereich von Aufgaben

Der *Gültigkeitsbereich einer Aufgabe* ist der Satz von Geräten, auf denen die Aufgabe ausgeführt wird. Es gibt folgende Arten von Gültigkeitsbereichen:

- Für eine *lokale Aufgabe* ist der Gültigkeitsbereich das Gerät selbst.
- Für eine *Aufgabe des Administrationsservers* ist der Gültigkeitsbereich der Administrationsserver.
- Für eine *Gruppenaufgabe* ist der Gültigkeitsbereich die Liste der Geräte, die in der Gruppe enthalten sind.

Beim Erstellen einer *globalen Aufgabe* können Sie die folgenden Methoden verwenden, um ihren Gültigkeitsbereich festzulegen:

- Bestimmte Geräte manuell festlegen.

  Als Adresse des Geräts können Sie eine IP-Adresse (oder einen IP-Bereich), den NetBIOS- oder den DNS-Namen verwenden.

- Geräteliste aus einer txt-Datei mit den hinzuzufügenden Geräteadressen importieren (jede Adresse muss in einer eigenen Zeile stehen).

  Wenn Sie eine Geräteliste aus einer Datei importieren oder eine Liste manuell erstellen, und wenn die Geräte namentlich identifiziert werden, darf die Liste nur Geräte enthalten, deren Daten bereits in die Datenbank des Administrationsservers eingegeben wurden. Darüber hinaus müssen die Informationen entweder während einer bestehenden Verbindung der Geräte oder während einer Gerätesuche eingegeben worden sein.

- Geräteauswahl angeben.

Im Laufe der Zeit ändert sich der Gültigkeitsbereich der Aufgabe, je nachdem, wie sich die Anzahl der Geräte ändert, die zur Auswahl gehören. Die Geräteauswahl kann aufgrund der Geräte-Attribute, einschließlich aufgrund der auf dem Gerät installierten Software, und aufgrund der dem Gerät zugewiesenen Tags strukturiert sein. Die Geräteauswahl ist die flexibelste Art zum Festlegen des Gültigkeitsbereichs einer Aufgabe.

Aufgaben für die Geräteauswahlen werden immer nach Zeitplan durch den Administrationsserver ausgeführt. Solche Aufgaben werden auf Geräten, die keine Verbindung mit dem Administrationsserver haben, nicht ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden direkt auf Geräten ausgeführt und sind daher nicht von der Geräteverbindung zum Administrationsserver abhängig.

Aufgaben für Geräteauswahlen werden nicht nach der lokalen Uhrzeit des Geräts, sondern nach der lokalen Uhrzeit des Administrationsservers ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden nach der lokalen Uhrzeit eines Geräts ausgeführt.

Aufgaben erstellen

So erstellen Sie eine Aufgabe:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie seinen Anweisungen.

3. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

4. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

So erstellen Sie eine neue Aufgabe, die ausgewählten Geräten zugewiesen wird:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Aktivieren Sie in der Liste der verwalteten Geräte die Kontrollkästchen neben den Geräten, auf denen die Aufgabe ausgeführt werden soll. Sie können die Such- und Filterfunktionen verwenden, um die gewünschten Geräte zu finden.

3. Klicken Sie auf die Schaltfläche **Aufgabe starten** und wählen Sie anschließend **Neue Aufgabe hinzufügen** aus.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.

   Im ersten Schritt des Assistenten können Sie die ausgewählten Geräte entfernen, die für den Gültigkeitsbereich der Aufgabe ausgewählt waren. Folgen Sie den Anweisungen des Assistenten.

4. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Die Aufgabe wird für die ausgewählten Geräte erstellt.

Aufgaben manuell starten

Die Anwendung startet Aufgaben gemäß den Zeitplaneinstellungen, die in den Eigenschaften der einzelnen Aufgaben angegeben sind. Sie können die Aufgabe jederzeit manuell aus der Aufgabenliste starten. Alternativ können Sie in der Liste **Verwaltete Geräte** die gewünschten Geräte auswählen und anschließend eine vorhandene Aufgabe für diese starten.

So starten Sie eine Aufgabe manuell:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Aktivieren Sie in der Aufgabenliste das Kontrollkästchen neben der Aufgabe, die Sie starten möchten.
3. Klicken Sie auf die Schaltfläche **Starten**.

   Die Aufgabe wird gestartet. Sie können den Status der Aufgabe in der Spalte **Status** oder durch Anklicken der Schaltfläche **Ergebnis** überprüfen.

Aufgabenliste anzeigen

Sie können die Liste der Aufgaben anzeigen, die in Kaspersky Security Center erstellt wurden.

Um die Liste der Aufgaben anzuzeigen:

Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

Die Aufgabenliste wird angezeigt. Die Aufgaben sind nach den Namen der Programme gruppiert, auf die sie sich beziehen. Beispiele: Die Aufgabe *Remote-Deinstallation eines Programms* bezieht sich auf den Administrationsserver, und die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* bezieht sich auf den Administrationsagenten.

Um die Eigenschaften einer Aufgabe anzuzeigen,

Klicken Sie auf den Namen der Aufgabe.

Das Fenster mit den Aufgabeneigenschaften enthält mehrere benannte Registerkarten. Zum Beispiel wird der **Aufgabentyp** auf der Registerkarte **Allgemein** angezeigt und der Aufgabenzeitplan auf der Registerkarte **Zeitplan**.

Allgemeine Aufgabeneinstellungen

Dieser Abschnitt enthält die Einstellungen, die Sie für Aufgaben anzeigen und konfigurieren können. Die Liste der verfügbaren Einstellungen hängt von der Aufgabe ab, die Sie konfigurieren.

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- Neustart-Einstellungen des Betriebssystems:

  - **Gerät nicht neu starten**

    Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

  - **Gerät neu starten**

    Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

  - **Benutzer fragen**

    Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

    Diese Option ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen nach (Min.)**

    Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

    Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neu starten nach (Min.)**

    Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

    Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  - **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

    Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

    Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

Diese Option ist standardmäßig deaktiviert.

- Zeitplaneinstellungen für Aufgaben:

  Die Arten des Zeitplans können je nach Aufgabe variieren.

  - **Einstellung Aufgabe starten:**

    - **Alle n Stunden**

      Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

      Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

    - **Alle n Tage**

      Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

      Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

    - **Alle n Minuten**

      Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

      Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

    - **Nach Wochentagen**

      Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

      Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

    - **Monatlich**

      Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

      In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

      Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

    - **Manuell**

      Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

      Diese Variante ist standardmäßig ausgewählt.

    - **Einmal**

      Die Aufgabe wird einmal zum angegebenen Datum und zur angegebenen Uhrzeit ausgeführt (standardmäßig entspricht dies dem Tag, an dem die Aufgabe erstellt wurde).

- **Sofort**

  Die Aufgabe wird nach dem Speichern der Einstellungen umgehend ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Nach dem Download von Updates in die Datenverwaltung**

  Die Aufgabe wird gestartet, nachdem Updates in die Datenverwaltung heruntergeladen wurden. Sie können diesen Zeitplan beispielsweise zur Suchen nach Suche nach Schwachstellen und erforderlichen Updates verwenden.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Abschluss einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

- Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
- Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

  Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
- Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

- Geräte, denen die Aufgabe zugewiesen wird:

  - **Geräte auswählen, die vom Administrationsserver erkannt wurden**

    Die Aufgabe wird einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

    Sie können diese Option beispielsweise für eine Aufgabe zur Installation des Administrationsagenten auf nicht zugeordneten Geräten verwenden.

- **Geräteadressen manuell angeben oder aus Liste importieren**

  Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

  Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

- **Aufgabe einer Administrationsgruppe zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

  Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

  Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

- Benutzerkonto-Einstellungen:

  - **Standardbenutzerkonto**

    Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

    Diese Variante ist standardmäßig ausgewählt.

  - **Benutzerkonto angeben**

    Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

  - **Benutzerkonto**

    Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

  - **Kennwort**

    Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

Einstellungen, die nach der Aufgabenerstellung festgelegt werden

Sie können die folgenden Einstellungen erst festlegen, nachdem eine Aufgabe erstellt wurde.

- Einstellungen der Gruppenaufgabe:

  - **Auf Untergruppen verteilen**

    Diese Option ist nur in den Einstellungen der Gruppenaufgaben verfügbar.

    Wenn diese Option aktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe die folgenden Objekte:

    - Die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.
    - Die Administrationsgruppen, die der ausgewählten Administrationsgruppe entsprechend der Gruppenhierarchie auf beliebiger Ebene untergeordnet sind.

    Wenn diese Option deaktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe nur die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.

    Diese Option ist standardmäßig aktiviert.

  - **An sekundäre und virtuelle Administrationsserver verteilen**

    Wenn diese Option aktiviert ist, wird die Aufgabe, die auf dem primären Administrationsserver wirksam ist, auch auf den sekundären Administrationsservern (einschließlich virtuellen) angewendet. Wenn auf dem sekundären Administrationsserver bereits eine Aufgabe des gleichen Typs existiert, werden auf dem sekundären Administrationsserver beide Aufgaben angewendet – die bestehende und die vom primären Administrationsserver übernommene.

    Diese Option ist nur verfügbar, wenn die Option **Auf Untergruppen verteilen** aktiviert ist.

    Diese Option ist standardmäßig deaktiviert.

- Erweiterte Zeitplaneinstellungen:

  - **Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren**

    Das Betriebssystem auf dem Gerät startet zum angegebenen Zeitpunkt, bevor die Aufgabe gestartet wird. Standardmäßig beträgt die Zeitspanne fünf Minuten.

    Aktivieren Sie diese Option, wenn Sie möchten, dass die Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich ausgeführt wird, einschließlich jener Geräte, die ausgeschaltet sind, wenn die Aufgabe gestartet werden soll.

    Wenn das Gerät nach Abschluss der Aufgabe automatisch ausgeschaltet werden soll, aktivieren Sie die Option **Geräte nach Abschluss der Aufgabe herunterfahren**. Die Option befindet sich im selben Fenster.

    Diese Option ist standardmäßig deaktiviert.

  - **Geräte nach Abschluss der Aufgabe herunterfahren**

    Sie können diese Option beispielsweise für eine Aufgabe zur Installation von Updates aktivieren, die Updates für Client-Geräte jeden Freitag nach Geschäftsschluss installiert und diese Geräte dann über das Wochenende abschaltet.

    Diese Option ist standardmäßig deaktiviert.

- **Aufgabe unterbrechen, wenn deren Ausführung länger dauert als**

  Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

- Benachrichtigungseinstellungen:

  - Block **Ereignisdaten speichern**:

    - **In der Administrationsserver-Datenbank speichern für (Tage)**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich beziehen, werden auf dem Administrationsserver während der festgelegten Anzahl an Tagen gespeichert. Wenn diese Zeitspanne abgelaufen ist, werden die Informationen vom Administrationsserver gelöscht.

      Diese Option ist standardmäßig aktiviert.

    - **Im System-Ereignisprotokoll des Geräts speichern**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe beziehen, werden lokal im Windows Ereignisprotokoll jedes Client-Geräts gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - **Im System-Ereignisprotokoll des Administrationsservers speichern**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich beziehen, werden zentral im Windows Ereignisprotokoll des Betriebssystems des Administrationsservers gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - **Alle Ereignisse speichern**

      Wenn diese Option ausgewählt ist, werden alle Ereignisse, die sich auf die Aufgabe beziehen, in den Ereignisprotokollen gespeichert.

    - **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**

      Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

    - **Nur die Ergebnisse der Aufgabenausführung speichern**

      Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Ergebnisse der Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

  - **Den Administrator über Ergebnisse der Aufgabenausführung benachrichtigen**

    Sie können die Methoden auswählen, über die Administratoren Benachrichtigungen über Ergebnisse der Aufgabenausführung erhalten: per E-Mail, mit SMS und durch Start einer ausführbaren Datei. Um die Benachrichtigungen zu konfigurieren, klicken Sie auf den Link **Einstellungen**.

Standardmäßig sind alle Methoden der Zustellung von Benachrichtigungen deaktiviert.

- **Nur über Fehler benachrichtigen**

  Wenn diese Option aktiviert ist, werden Administratoren nur dann benachrichtigt, wenn die Aufgabenausführung mit einem Fehler beendet wird.

  Wenn diese Option deaktiviert ist, werden Administratoren nach jeder Aufgabenausführung benachrichtigt.

  Diese Option ist standardmäßig aktiviert.

- Sicherheitseinstellungen.

- Einstellungen für den Gültigkeitsbereich der Aufgabe.

  Abhängig davon, wie der Gültigkeitsbereich der Aufgabe bestimmt wird, sind die folgenden Einstellungen verfügbar:

  - **Geräte**

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Administrationsgruppe bestimmt wird, können Sie diese Gruppe anzeigen. Hier sind keine Änderungen möglich. Sie können aber **Ausschlüsse vom Gültigkeitsbereich der Aufgabe** festlegen.

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Liste von Geräten bestimmt wird, können Sie diese Liste ändern, indem Sie Geräte hinzufügen und entfernen.

  - **Geräteauswahl**

    Sie können die Geräteauswahl ändern, für welche die Aufgabe übernommen wird.

  - **Ausschlüsse vom Gültigkeitsbereich der Aufgabe**

    Sie können Gruppen von Geräten festlegen, für welche die Aufgabe nicht angewendet wird. Gruppen, die ausgeschlossen werden sollen, können sich nur den Untergruppen der Administrationsgruppe befinden, für welche die Aufgabe übernommen wird.

- **Revisionsverlauf**.

Aufgaben exportieren

Mit Kaspersky Security Center können Sie eine Aufgabe und deren Einstellungen in einer klt-Datei speichern. Sie können diese klt-Datei verwenden, um sowohl in Kaspersky Security Center Windows als auch in Kaspersky Security Center Linux die gespeicherte Aufgabe zu importieren.

Um eine Aufgabe zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Aktivieren Sie das Kontrollkästchen neben der Aufgabe, die Sie exportieren möchten.

   Sie können nicht mehrere Aufgaben gleichzeitig exportieren. Wenn Sie mehr als eine Aufgabe auswählen, wird die Schaltfläche **Exportieren** deaktiviert. Die Aufgaben des Administrationsservers sind für den Export ebenfalls nicht verfügbar.
3. Klicken Sie auf die Schaltfläche **Exportieren**.

4. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Aufgabendatei an. Klicken Sie auf **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Aufgabendatei automatisch im Ordner **Downloads** gespeichert.

Aufgaben importieren

Mit Kaspersky Security Center können Sie eine Aufgabe aus einer klt-Datei importieren. Die klt-Datei enthält die exportierte Aufgabe und deren Einstellungen.

Um eine Aufgabe zu importieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Importieren**.
3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Aufgabendatei auszuwählen, die Sie importieren möchten.
4. Geben Sie im folgenden Fenster den Pfad zur klt-Aufgabendatei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Aufgabendatei auswählen können.

   Die Verarbeitung der Aufgabe beginnt.
5. Nachdem die Aufgabe erfolgreich verarbeitet wurde, wählen Sie die Geräte aus, denen Sie die Aufgabe zuweisen möchten. Wählen Sie dazu eine der folgenden Optionen aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

     Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

6. Wählen Sie den Gültigkeitsbereich der Aufgabe aus.

7. Klicken Sie auf die Schaltfläche **Abgeschlossen**, um den Import der Aufgabe abzuschließen.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Aufgabe erfolgreich importiert wurde, können klicken Sie auf den Link **Details**, um die Eigenschaften der Aufgabe anzuzeigen.

Nach einem erfolgreichen Import wird die Aufgabe in der Liste der Aufgaben angezeigt. Die Einstellungen und der Zeitplan der Aufgabe werden ebenfalls importiert. Die Aufgabe wird gemäß ihrem Zeitplan gestartet.

Wenn die neu importierte Aufgabe einen identischen Namen wie eine bereits vorhandene Aufgabe hat, wird der Name der importierten Aufgabe um den Index **(<nächste Sequenznummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Assistent zum Ändern der Aufgabenkennwörter starten

Für eine nicht lokale Aufgabe können Sie ein Benutzerkonto angeben, unter dem die Aufgabe ausgeführt werden soll. Sie können das Benutzerkonto bei der Aufgabenerstellung oder in den Eigenschaften einer vorhandenen Aufgabe angeben. Wenn das angegebene Benutzerkonto den Sicherheitsvorschriften des Unternehmens unterliegt, müssen Sie das Benutzerkonto-Kennwort möglicherweise von Zeit zu Zeit ändern. Wenn das Benutzerkonto-Kennwort abläuft und Sie ein neues festlegen, müssen Sie das neue gültige Kennwort in den Aufgabeneigenschaften angeben, damit die Aufgaben korrekt starten können.

Mit dem Assistenten zum Ändern der Aufgabenkennwörter können Sie das alte Kennwort in allen Aufgaben, in denen das Benutzerkonto angegeben ist, automatisch durch das neue Kennwort ersetzen. Alternativ können Sie das Kennwort auch manuell in den Eigenschaften der einzelnen Aufgaben ändern.

Um den Assistenten zum Ändern der Aufgabenkennwörter zu starten:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **Benutzerkonto-Anmeldedaten für den Aufgabenstart verwalten**.

Folgen Sie den Anweisungen des Assistenten.

Schritt 1. Anmeldedaten angeben

Geben Sie die neuen Anmeldedaten an, die momentan in Ihrem System gültig sind (z. B. in Active Directory). Wenn Sie zum nächsten Schritt des Assistenten wechseln, überprüft Kaspersky Security Center, ob der angegebene Benutzerkonto-Name mit dem Benutzerkonto-Namen in den Eigenschaften der einzelnen nicht lokalen Aufgaben übereinstimmt. Stimmen die Benutzerkonto-Namen überein, so wird das Kennwort in den Aufgabeneigenschaften automatisch durch das neue ersetzt.

Um das neue Konto anzugeben, wählen Sie eine Option aus:

- **Aktuelles Benutzerkonto verwenden**

  Der Assistent verwendet den Namen des Kontos, unter dem Sie derzeit bei Kaspersky Security Center Web Console angemeldet sind. Geben Sie dann manuell das Kontokennwort in dem Feld **Aktuelles Kennwort für die Verwendung in Aufgaben** ein.

- **Anderes Benutzerkonto angeben**

  Geben Sie den Namen des Kontos an, unter dem die Aufgaben gestartet werden sollen. Geben Sie dann das Kontokennwort in dem Feld **Aktuelles Kennwort für die Verwendung in Aufgaben** ein.

Wenn Sie das Feld **Vorheriges Kennwort (optional; wenn Sie es durch das Aktuelle ersetzen wollen)** ausfüllen, ersetzt Kaspersky Security Center das Kennwort nur für jene Aufgaben, in denen sowohl der Benutzerkonto-Name als auch das alte Kennwort gefunden werden. Das Ersetzen erfolgt automatisch. In allen übrigen Fällen müssen Sie eine Aktion auswählen, die beim nächsten Schritt des Assistenten ausgeführt werden soll.

Schritt 2. Auszuführenden Vorgang auswählen

Wenn Sie beim ersten Schritt des Assistenten das alte Kennwort nicht angegeben haben oder das angegebene alte Kennwort nicht mit den Kennwörtern in den Aufgabeneigenschaften übereinstimmt, müssen Sie eine Aktion auswählen, die für die gefundenen Aufgaben ausgeführt werden soll.

So wählen Sie eine Aktion für eine Aufgabe aus:

1. Aktivieren Sie das Kontrollkästchen neben der Aufgabe, für die Sie eine Aktion wählen möchten.
2. Führen Sie eine der folgenden Optionen aus:

   - Um das Kennwort in den Aufgabeneigenschaften zu entfernen, klicken Sie auf **Anmeldedaten löschen**.

     Die Aufgabe wird so angepasst, dass sie unter dem Standardkonto ausgeführt wird.

   - Um das Kennwort durch das neue zu ersetzen, klicken Sie auf **Die Änderung des Kennworts erzwingen, selbst wenn das alte Kennwort falsch oder nicht angegeben ist**.

   - Um die Kennwortänderung abzubrechen, klicken Sie auf **Es ist keine Aktion ausgewählt**.

   Die ausgewählten Aktionen werden angewendet, wenn Sie zum nächsten Schritt des Assistenten gewechselt sind.

Schritt 3. Ergebnisse anzeigen

Zeigen Sie beim letzten Schritt des Assistenten die Ergebnisse die einzelnen gefundenen Aufgaben an. Klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.

Aufgabe zur Remote-Ausführung von Skripten erstellen

Sie können die Aufgabe *Skripte remote ausführen* erstellen, um auf einem Client-Gerät ein Installationspaket auszuführen und eine Anwendung per Fernzugriff zu installieren.

Ein Installationspaket enthält ein zip-Archiv mit einer Reihe von Skripten zur Ausführung auf Client-Geräten sowie die Datei "manifest.json". Weitere Informationen zum Erstellen eines solchen Installationspakets finden Sie in diesem Artikel.

Diese Aufgabe kann nur auf Geräten mit dem Administrationsagenten für Linux gestartet werden.

So starten Sie die Aufgabe Skripte remote ausführen:

1. Gehen Sie zum **Assistent für das Erstellen einer Aufgabe** und wählen Sie den Aufgabentyp **Skripte remote ausführen** aus.

2. Geben Sie den Aufgabennamen ein und wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll. Klicken Sie auf **Weiter**.

3. Wählen Sie ein Installationspaket zur Remote-Ausführung aus, das auf einem zip-Archiv basiert und die Datei "manifest.json" enthält.

   Wenn Sie nicht möchten, dass die Aufgabe auf Geräten, auf denen sie bereits abgeschlossen wurde, erneut ausgeführt wird, aktivieren Sie die Option **Diese Aufgabe nicht auf Geräten ausführen, auf denen sie bereits abgeschlossen wurde**.

4. Wählen Sie ein Benutzerkonto aus, unter dem die Aufgabe ausgeführt wird.

   Wenn Sie das Standardkonto auswählen, wird die Aufgabe vom Administrationsagenten (Root-Benutzerkonto) ausgeführt.

   > Sobald die Aufgabe *Skripte remote ausführen* gestartet wurde, können Sie das ihr zugewiesene Benutzerkonto nicht mehr ändern. Um das Benutzerkonto für diese Aufgabe zu ändern, beenden Sie die Aufgabe in den Aufgabeneinstellungen und starten Sie sie anschließend mit den korrekten Einstellungen erneut.

5. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

6. Klicken Sie auf **Fertigstellen**.

   Die Aufgabe *Remote-Ausführung von Skripten* wird erstellt und in der Aufgabenliste angezeigt.

> Nachdem die Daten von der Aufgabe *Remote-Ausführung von Skripten* empfangen wurden, beschränkt der Administrationsagent den Zugriff auf die abgerufenen Daten für alle Benutzer, mit Ausnahme des Administrators und des in den Aufgabeneinstellungen angegebenen Benutzers.

Anwendungen mittels Aufgabe zur Remote-Ausführung von Skripten auf Geräten installieren

Die Aufgabe *Skripte remote ausführen* kann dazu verwendet werden, eine Anwendung auf einem Client-Gerät per Fernzugriff zu installieren. Dazu wird ein benutzerdefiniertes Installationspaket erstellt.

In diesem Artikel erfahren Sie, wie Sie ein Archiv für diese Aufgabe vorbereiten.

Um ein Installationspaket für die Remote-Installation einer Anwendung auf einem Client-Gerät zu erstellen, muss das Archiv, das Sie für diese Aufgabe hochladen möchten, die folgenden Dateien enthalten:

- `<Paketname>.deb`
- **install.sh**

```
sudo apt-get install <Paketname>.deb
```

- **manifest.json**

JSON-Schema für die Remote-Installation einer Anwendung

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<bei Bedarf Argumente eingeben>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

Beschreibung der Arrays

1. `version` – Version der Manifestdatei und der Aufgabe.

   Derzeit ist der einzig gültige Wert "1".

2. Die Elemente des Arrays `actions` bestimmen den Aufbau und die Reihenfolge der Skripte, die in der Aufgabe ausgeführt werden.

   Die Ausführungsreihenfolge des Skripts entspricht dem Index (Platz) eines Elements im Array.

3. Für jedes Element des Arrays `actions` sind die folgenden Elemente definiert.

   a. `type` – Typ des ausführbaren Befehls aus Skripten. Derzeit ist der Wert stets `execute`.

   b. `path` – Pfad zur Skriptdatei im Archiv.

   c. `args` – Argumente, die als Teil des ausführbaren Befehls an das Skript übertragen werden.

   d. `results` – Array, das abhängig vom Ergebnis der Aufgabe weitere Aktionen definiert.

      1. `code` – Wert, den ein Skript zurückgibt.

      2. `next` – Aktion, die als nächste ausgeführt werden soll. Die Aktion `continue` führt zur Ausführung des nächsten Skripts (Element im Array `actions`) und die Aktion `break` hält die Aufgabe an.

   e. `default_next` – Aktion, wenn ein Skript einen Wert zurückgibt, der nicht in `results` enthalten ist.

Wenn die Aufgabe *Skripte remote ausführen* gestartet wird, lädt der Administrationsagent das Installationspaket mit der Anwendung auf das Client-Gerät hoch. Wenn das Client-Gerät das Installationspaket empfängt, analysiert der Administrationsagent auf diesem Gerät die Datei "manifest.json". Abhängig vom Ergebnis legt der Administrationsagent die Ausführungsreihenfolge der Skripte und Aktionen fest und startet anschließend die Ausführung.

Nach Abschluss der Aufgabe *Skripte remote ausführen* ist die Anwendung auf dem Client-Gerät installiert.

Benachrichtigungen und Überwachung für die Aufgabe zur Remote-Ausführung von Skripten konfigurieren

Für die Aufgabe *Skripte remote ausführen* können Sie die Überwachung, das Verhalten zur Speicherung von Ereignissen und die Benachrichtigungen konfigurieren.

So zeigen Sie den Status der Aufgabe Skripte remote ausführen an:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
   Die Aufgabenliste wird angezeigt.
2. Wählen Sie die Aufgabe aus und klicken Sie auf **Geräteverlauf**.
   Der Aufgabenfortschritt wird angezeigt.

So konfigurieren Sie das Verhalten zur Speicherung von Ereignissen:

1. Klicken Sie in der Aufgabenliste auf die Aufgabe und gehen Sie zur Registerkarte **Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungen** auf **Einstellungen**.
3. Wählen Sie aus, wie sich die Anwendung nach Abschluss der Aufgabe verhalten soll:
   - **Alle Ereignisse speichern**.
   - **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**.
   - **Nur die Ergebnisse der Aufgabenausführung speichern**.
     Die Ereignisse werden im **Geräteverlauf** und in der **Ereignis-Datenverwaltung** gespeichert.
     Standardmäßig werden nur die Ergebnisse der Aufgabenausführung gespeichert.

     > Wenn Sie **Alle Ereignisse speichern** auswählen, werden nur die Ergebnisse der Aufgabenausführung gespeichert.
4. Wenn Sie die Ereignisse in der Administrationsserver-Datenbank, im Ereignisprotokoll auf dem Administrationsserver oder auf dem Gerät behalten möchten, aktivieren Sie die entsprechende Option.

Weitere Informationen über die Konfiguration von Benachrichtigungen finden Sie in diesem Artikel.

Archiv für die Aufgabe zur Remote-Ausführung von Skripten vorbereiten

Ein Archiv für die Aufgabe *Skripte remote ausführen* auf Grundlage einer manifest.json-Datei muss die folgenden Anforderungen erfüllen:

- Archivformat: zip.
- Gesamtgröße: maximal 1 GB.
- Die Anzahl der Dateien und Ordner im Archiv ist unbegrenzt.

- Die Manifestdatei des Archivs muss dem unten aufgeführten Schema entsprechen und den Namen "manifest.json" haben. Das Schema wird erst während der Aufgabenausführung auf einem Gerät validiert.

  JSON-Schema der Manifestdatei und Beschreibung der Arrays

  JSON-Schema

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
```

```
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Beispiel für die Manifestdatei

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- Das Archiv muss folgende Struktur besitzen:

  `manifest.json`

  `<file1>`

<file2>

<folder1>/<file3>

<folder2>/<folder3>/<file4>

...

<fileX>

Die Datei "manifest.json" ist die Manifestdatei für die Aufgabe.

<file1>, ..., <fileX> entspricht den Dateien mit auszuführenden Skripten.

Installationspaket auf Basis einer Manifestdatei erstellen

So erstellen Sie ein Installationspaket auf Grundlage einer Manifestdatei:

1. Führen Sie eine der folgenden Aktionen aus:

   - Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für neue Installationspakete wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.

3. Wählen Sie die Option **Installationspaket auf Basis eines zip-Archivs mit der Datei "manifest.json" für die Aufgabe zur Remote-Ausführung von Skripten erstellen** aus.

4. Geben Sie den Namen des Pakets an und klicken Sie auf **Durchsuchen**.

   In Ihrem Browser wird das Windows-Standardfenster **Öffnen** geöffnet. Dort können Sie eine Datei zum Erstellen des Installationspakets auswählen.

5. Wählen Sie eine Archivdatei aus, die sich auf einem verfügbaren Datenträger befindet. In diesem Artikel erfahren Sie, wie Sie ein Archiv für diese Aufgabe vorbereiten.

   Es wird damit begonnen, die Datei auf den Kaspersky Security Center Administrationsserver hochzuladen.

   Das Erstellen des Installationspakets wird gestartet.

   Der Assistent meldet, wenn der Vorgang abgeschlossen ist.

   Falls das Installationspaket nicht erstellt wurde, wird eine entsprechende Meldung angezeigt.

6. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Assistenten zu schließen.

Das von Ihnen erstellte Installationspaket wird in den Unterordner "Pakete" des Freigegebenen Ordners des Administrationsservers heruntergeladen. Nach dem Herunterladen erscheint das Installationspaket in der Liste der Installationspakete.

Wenn Sie in der Liste der auf dem Administrationsserver verfügbaren Installationspakete auf den Link mit dem Namen eines benutzerdefinierten Installationspakets klicken, haben Sie folgende Optionen:

- Die folgenden Eigenschaften eines Installationspakets anzeigen:
  - **Name.** Der Name des benutzerdefinierten Installationspakets.
  - **Quelle.** Hersteller der Anwendung.
  - **Version.** Version der Anwendung.
  - **Erstellt.** Erstellungsdatum des Installationspakets.
  - **Geändert.** Änderungsdatum des Installationspakets.
  - **Pfad.** Pfad des benutzerdefinierten Installationspakets auf dem Administrationsserver.
- Paketname und Befehlszeilenparameter ändern. Diese Funktion ist nur für Pakete verfügbar, die nicht auf Grundlage von Kaspersky-Anwendungen erstellt wurden.

Client-Geräte verwalten

Mit Kaspersky Security Center können Sie Client-Geräte verwalten:

- Einstellungen und Status von verwalteten Geräten anzeigen, einschließlich Clustern und Server-Arrays.
- Verteilungspunkte konfigurieren.
- Aufgaben verwalten.

Sie können Administrationsgruppen verwenden, um Client-Geräte zu einem Satz zusammenzufassen, der als eine einzige Einheit verwaltet werden kann. Ein Client-Gerät kann nur in einer Administrationsgruppe enthalten sein. Geräte können auf der Grundlage von **Regelbedingungen** automatisch einer Gruppe zugewiesen werden:

- Regeln für das Verschieben von Geräten erstellen.
- Regeln für das Verschieben von Geräten kopieren.
- Bedingungen für eine Verschiebungsregel für Geräte.

Sie können Geräteauswahlen verwenden, um Geräte basierend auf einer Bedingung zu filtern. Sie können auch Geräte markieren, um eine Auswahl zu erstellen, Geräte zu finden und Geräte auf Administrationsgruppen zu verteilen.

Einstellungen eines verwalteten Geräts

So zeigen Sie die Einstellungen eines verwalteten Geräts an:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des entsprechenden Geräts.

Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

Im oberen Bereich des Eigenschaftenfensters werden die folgenden Registerkarten mit den wichtigsten Einstellungsgruppen angezeigt:

- **Allgemein**

  Diese Registerkarte umfasst die folgenden Abschnitte:

  - Der Abschnitt **Allgemein** enthält allgemeine Informationen über das Client-Gerät. Die Informationen beruhen auf Daten, die bei der letzten Synchronisierung des Client-Geräts mit dem Administrationsserver empfangen wurden:

    - **Name**

      In diesem Feld steht der Name des Client-Geräts in der Administrationsgruppe und der Name kann geändert werden.

    - **Beschreibung**

      In diesem Feld können Sie eine zusätzliche Beschreibung für das Client-Gerät eingeben.

    - **Gerätestatus**

      Status des Client-Geräts, der ihm anhand der vom Administrator festgelegten Kriterien den Status des Antiviren-Schutzes und der Aktivität des Geräts im Netzwerk zugewiesen wird.

    - **Vollständiger Gruppenname**

      Administrationsgruppe, zu der das Client-Gerät gehört.

    - **Letzte Aktualisierung der Antiviren-Datenbanken**

      Datum des letzten Updates der Antiviren-Datenbanken oder der Anwendungen auf dem Gerät.

    - **Verbindung mit dem Administrationsserver**

      Datum und Uhrzeit der letzten Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver.

    - **Zuletzt im Netzwerk sichtbar**

      Zeitpunkt (Datum und Uhrzeit), zu dem das Gerät zuletzt im Netzwerk gesehen wurde.

    - **Version des Administrationsagenten**

      Version des installierten Administrationsagenten.

- **Erstellt**

  Datum der Geräte-Erstellung innerhalb von Kaspersky Security Center.

- **Gerätebesitzer**

  Name des Gerätebesitzers. Sie können einen Benutzer als Gerätebesitzer zuweisen oder entfernen, indem Sie auf den Link **Gerätebesitzer verwalten** klicken.

- **Verbindung mit Administrationsserver nicht trennen**

  Wenn diese Option aktiviert ist, wird die dauerhafte Verbindung zwischen dem verwalteten Gerät und dem Administrationsserver aufrecht erhalten. Sie können diese Option verwenden, wenn Sie keine Push-Server einsetzen, die eine solche Verbindung bereitstellen.

  Wenn diese Option deaktiviert ist und keine Push-Server verwendet werden, verbindet sich das verwaltete Gerät nur zur Datensynchronisierung oder Datenübertragung mit dem Administrationsserver.

  Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

  Diese Option ist auf verwalteten Geräten standardmäßig deaktiviert. Diese Option ist auf dem Gerät, auf dem der Administrationsserver installiert ist, standardmäßig aktiviert und bleibt selbst dann aktiviert, wenn Sie versuchen, sie zu deaktivieren.

- Der Abschnitt **Netzwerk** enthält folgende Informationen zu den Netzwerkeinstellungen des Client-Geräts:

  - **IP-Adresse**

    IP-Adresse des Geräts.

  - **Windows-Domäne**

    Windows-Domäne oder Arbeitsgruppe, zu der das Gerät gehört.

  - **DNS-Name**

    Name der DNS-Domäne des Client-Geräts.

  - **NetBIOS-Name**

    Name des Client-Geräts im Windows-Netzwerk.

  - **IPv6-Adresse**

- Der Abschnitt **System** enthält Daten zum Betriebssystem, das auf dem Client-Gerät installiert ist:

  - **Betriebssystem**

  - **CPU-Architektur**

  - **Gerätename**

  - **Typ der virtuellen Maschine**

    Hersteller der virtuellen Maschine.

  - **Dynamische virtuelle Maschine als Teil von VDI**

Diese Zeile gibt an, ob das Client-Gerät eine dynamische virtuelle Maschine als Teil einer VDI ist.

- Der Abschnitt **Schutz** enthält folgende Informationen über den Status des Antiviren-Schutzes auf dem Client-Gerät:

  - **Sichtbar**

    Sichtbarkeitsstatus des Client-Geräts.

  - **Gerätestatus**

    Status des Client-Geräts, der ihm anhand der vom Administrator festgelegten Kriterien den Status des Antiviren-Schutzes und der Aktivität des Geräts im Netzwerk zugewiesen wird.

  - **Statusbeschreibung**

    Status des Schutzes für das Client-Gerät und der Verbindung zum Administrationsserver.

  - **Schutzstatus**

    Dieses Feld zeigt den aktuellen Status des Echtzeitschutzes auf dem Client-Gerät an.

    Wenn sich der Status auf dem Gerät ändert, wird der neue Status erst im Eigenschaftenfenster des Geräts angezeigt, nachdem das Client-Gerät mit dem Administrationsserver synchronisiert wurde.

  - **Letzte vollständige Untersuchung**

    Datum und Uhrzeit der letzten Schadsoftware-Untersuchung auf einem Client-Gerät.

  - **Virus gefunden**

    Gesamtzahl der auf dem Client-Gerät gefundenen Bedrohungen seit der Installation der Sicherheitsanwendung (seit der ersten Untersuchung des Geräts) oder seit dem letzten Zurücksetzen des Zählers.

  - **Objekte, die nicht desinfiziert werden konnten**

    Anzahl der unverarbeiteten Dateien auf einem Client-Gerät.

    In diesem Feld wird die Anzahl der unverarbeiteten Dateien auf mobilen Geräten nicht berücksichtigt.

  - **Status der Datenträgerverschlüsselung**

    Aktueller Status der Verschlüsselung von Dateien auf den lokalen Laufwerken des Geräts. Eine Beschreibung der Statuswerte finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

- Im Abschnitt **Gerätestatus wird vom Programm bestimmt** werden Daten über den Gerätestatus, der durch das auf dem Gerät installierte verwaltete Programm bestimmt wird, angezeigt. Der Gerätestatus kann von dem durch Kaspersky Security Center vorgegebenen Status abweichen.

- **Programme**

  Diese Registerkarte listet alle Kaspersky-Anwendungen auf, die auf dem Client-Gerät installiert sind. Auf dieser Registerkarte befinden sich die Schaltflächen **Starten** und **Stoppen**, mit denen Sie erforderliche Kaspersky-Anwendungen (mit Ausnahme des Administrationsagenten) starten und stoppen können. Sie können diese Schaltflächen verwenden, wenn auf dem verwalteten Gerät der UDP-Port 15000 für den Empfang von Push-Benachrichtigungen vom Administrationsserver verfügbar ist. Wenn das verwaltete Gerät nicht für Push-Benachrichtigungen verfügbar ist, aber der Modus für die dauerhafte Verbindung mit dem Administrationsserver aktiviert ist (d. h., im Abschnitt **Allgemein** ist die Option **Verbindung mit Administrationsserver nicht trennen** aktiviert), stehen die Schaltflächen **Starten** und **Stoppen** auch zur Verfügung. Andernfalls wird beim Versuch, die Anwendung zu starten oder zu stoppen, eine Fehlermeldung ausgegeben. Sie können auch auf die Namen der Anwendungen klicken, um sich allgemeine Informationen über eine Anwendung, eine Liste mit allen auf dem Gerät aufgetretenen Ereignissen und die Einstellungen der Anwendung anzeigen zu lassen.

- **Aktive Richtlinien und Richtlinienprofile**

  Diese Registerkarte listet die Richtlinien und Richtlinienprofile auf, die dem verwalteten Gerät derzeit zugewiesen sind.

- **Aufgaben**

  Auf der Registerkarte **Aufgaben** können Sie die Aufgaben eines Client-Geräts verwalten: Liste der vorhandenen Aufgaben anzeigen, neue Aufgaben erstellen, Aufgaben entfernen, starten und beenden, Aufgabeneinstellungen ändern und die Ergebnisse der Aufgabenausführung anzeigen. Die Aufgabenliste beruht auf Daten, die während der letzten Synchronisierung des Clients mit dem Administrationsserver empfangen wurden. Die Daten über den Aufgabenstatus erhält der Administrationsserver vom Client-Gerät. Wenn auf dem verwalteten Gerät der UDP-Port 15000 für den Empfang von Push-Benachrichtigungen vom Administrationsserver verfügbar ist, werden der Aufgabenstatus angezeigt und die Schaltflächen zur Aufgabenverwaltung aktiviert. Wenn der Push-Server das verwaltete Gerät nicht erreichen kann, aber der Modus für die dauerhafte Verbindung mit dem Administrationsserver aktiviert ist (d. h., im Abschnitt **Allgemein** ist die Option **Verbindung mit Administrationsserver nicht trennen** aktiviert), stehen die Aktionen für die Aufgaben auch zur Verfügung.

  Wenn keine Verbindung besteht, wird kein Status angezeigt und die Schaltflächen sind nicht verfügbar.

- **Ereignisse**

  Die Registerkarte **Ereignisse** enthält die Ereignisse, die für das ausgewählte Client-Gerät auf dem Administrationsserver registriert wurden.

  Sie können die Ereignisse von Geräten exportieren, kopieren und löschen.

- **Sicherheitsprobleme**

  Auf der Registerkarte **Sicherheitsprobleme** können Sie Sicherheitsvorfälle für ein Client-Gerät anzeigen, bearbeiten oder erstellen. Sicherheitsvorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten verwalteten Kaspersky-Anwendungen als auch manuell vom Administrator erstellt werden. Wenn beispielsweise einige Benutzer immer wieder Schadsoftware von Wechseldatenträgern auf Geräte übertragen, kann der Administrator einen Sicherheitsvorfall erstellen. Der Administrator kann im Text des Sicherheitsvorfalls eine kurze Beschreibung des Falls bereitstellen und Aktionen vorschlagen (etwa Disziplinarmaßnahmen gegen einen Benutzer) und einen Link zum Benutzer oder zu den Benutzern hinzufügen.

  Ein Vorfall, für den alle erforderlichen Aktionen ausgeführt worden sind, wird als *Bearbeitet* bezeichnet. Das Vorhandensein von nicht bearbeiteten Sicherheitsvorfällen kann als Bedingung für eine Statusänderung des Geräts in *Kritisch* oder *Warnung* ausgewählt werden.

  Dieser Abschnitt enthält eine Liste der für das Gerät erstellten Sicherheitsvorfälle. Die Sicherheitsvorfälle werden nach Signifikanz und Art eingestuft. Die Art des Sicherheitsvorfalls wird von der Kaspersky-Anwendung bestimmt, die den Vorfall erstellt hat. Bearbeitete Sicherheitsvorfälle können in der Liste durch Aktivieren des Kontrollkästchens in der Spalte **Bearbeitet** gekennzeichnet werden.

- **Tags**

  Auf der Registerkarte **Tags** können Sie die Liste der Schlüsselwörter verwalten, auf deren Grundlage die Suche nach Client-Geräten ausgeführt wird: Liste der vorhandenen Tags anzeigen, Tags aus der Liste zuweisen, Regeln für die automatische Zuweisung von Tags konfigurieren, neue Tags hinzufügen und alte Tags umbenennen sowie Tags löschen.

- **Erweitert**

  Diese Registerkarte umfasst die folgenden Abschnitte:

  - **Programm-Registry**. In diesem Abschnitt können Sie die Registry der auf dem Client-Gerät installierten Anwendungen und der Anwendungs-Updates anzeigen lassen und die Darstellung der Programm-Registry konfigurieren.

    Informationen über die installierten Anwendungen sind verfügbar, wenn der auf dem Client-Gerät installierte Administrationsagent die erforderlichen Daten an den Administrationsserver überträgt. Die Einstellungen für die Übertragung der Informationen an den Administrationsserver können Sie im Eigenschaftenfenster des Administrationsagenten oder seiner Richtlinie im Abschnitt **Datenverwaltung** anpassen.

    Durch Klicken auf einen Anwendungsnamen wird ein Fenster geöffnet, das die Anwendungsdetails und eine Liste der für die Anwendung installierten Update-Pakete enthält.

  - **Ausführbare Dateien**. Dieser Abschnitt enthält ausführbare Dateien, die auf dem Client-Gerät gefunden wurden.

  - **Verteilungspunkte**. Dieser Abschnitt enthält eine Liste der Verteilungspunkte, mit denen das Gerät interagiert.

    - **In Datei exportieren**

      Mithilfe der Schaltfläche **In Datei exportieren** können Sie die Liste der Verteilungspunkte, mit denen das Gerät interagiert, in einer Datei speichern. Standardmäßig exportiert die Anwendung die Liste der Geräte in eine Datei im csv-Format.

    - **Eigenschaften**

      Mithilfe der Schaltfläche **Eigenschaften** können Sie die Einstellungen der Verteilungspunkte, mit denen das Gerät interagiert, anzeigen und anpassen.

  - **Hardware-Register**. Dieser Abschnitt enthält Informationen zur Hardware, die auf dem Client-Gerät installiert ist.

    Wenn der Administrationsagent auf einem Windows-Gerät installiert ist, sendet er nur die folgenden Informationen über die Gerätehardware an den Administrationsserver:

    - Arbeitsspeicher
    - Massenspeichergeräte
    - Mainboard
    - Prozessor
    - Netzwerkadapter
    - Monitore

- Grafikkarte
- Soundkarte

Wenn der Administrationsagent auf einem Linux- oder macOS-Gerät installiert ist, sendet er die folgenden Informationen über die Gerätehardware an den Administrationsserver (vorausgesetzt, diese Information wird durch das Betriebssystem bereitgestellt):

- Gesamtgröße des Arbeitsspeichers
- Gesamtgröße der Massenspeicher
- Mainboard
- Prozessor
- Netzwerkadapter

- **Verfügbare Updates**. Dieser Abschnitt enthält eine Liste der auf dem Gerät gefundenen Programm-Updates, die noch nicht installiert wurden.

- **Schwachstellen in Programmen**. Dieser Abschnitt bietet Informationen über die Schwachstellen von Drittanbieter-Anwendung, die auf den Client-Geräten installiert sind.

  Um die Schwachstellen in einer Datei zu speichern, aktivieren Sie die Kontrollkästchen neben den betreffenden Schwachstellen und klicken Sie dann auf die Schaltfläche **In csv-Datei exportieren** oder **In txt-Datei exportieren**.

  Dieser Abschnitt enthält die folgenden Einstellungen:

  - **Nur Schwachstellen anzeigen, die geschlossen werden können**

    Ist diese Option aktiviert, werden in diesem Abschnitt jene Schwachstellen angezeigt, die durch einen Patch geschlossen werden können.

    Ist diese Option deaktiviert, werden in diesem Abschnitt sowohl Schwachstellen angezeigt, die durch einen Patch geschlossen werden können, als auch Schwachstellen, für die kein Patch vorhanden ist.

    Diese Option ist standardmäßig aktiviert.

  - **Schwachstellen-Eigenschaften**

    Wählen Sie in der Liste eine Software-Schwachstelle aus, um die Eigenschaften der ausgewählten Software-Schwachstelle in einem separaten Fenster anzuzeigen. In diesem Fenster sind folgende Aktionen möglich:

    - Schwachstellen in Programmen auf diesem verwalteten Gerät ignorieren (in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console).
    - Liste mit Korrekturen anzeigen, die für die Schwachstelle empfohlen werden.
    - Programm-Updates manuell angeben, um eine Schwachstelle zu beheben (in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console).
    - Schwachstellen-Instanzen anzeigen.
    - Liste der vorhandenen Aufgaben zur Schwachstellen-Behebung anzeigen und neue Aufgaben zur Schwachstellen-Behebung erstellen.

- **Remote-Diagnose**. In diesem Abschnitt können Sie die Ferndiagnose von Client-Geräten durchführen.

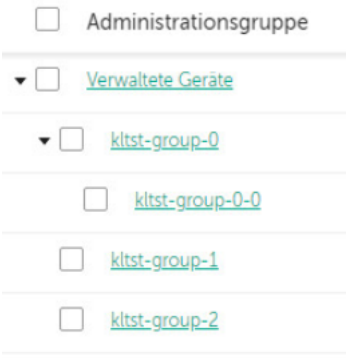
Wenn Sie PostgreSQL, MariaDB oder MySQL als DBMS verwenden, wird auf der Registerkarte **Ereignisse** möglicherweise eine unvollständige Liste der Ereignisse für das ausgewählte Client-Gerät angezeigt. Dies kommt vor, wenn das DBMS eine sehr große Anzahl von Ereignissen speichert. Sie können die Anzahl der angezeigten Ereignisse auf eine der folgenden Arten erhöhen:

- Nicht benötigte Ereignisse entfernen.
- Speicherdauer für nicht benötigte Ereignisse verkürzen.

Verwenden Sie die Berichte, um eine vollständige Liste der auf dem Administrationsserver für das Gerät protokollierten Ereignisse anzuzeigen.

Administrationsgruppen anlegen

Unmittelbar nach der Installation von Kaspersky Security Center enthält die Hierarchie der Administrationsgruppen nur eine Administrationsgruppe, die aufgerufen wird: **Verwaltete Geräte**. Wenn Sie eine Hierarchie der Administrationsgruppen erstellen, können Sie sowohl Geräte, inklusive virtueller Maschinen, als auch untergeordnete Gruppen zur Gruppe **Verwaltete Geräte** hinzufügen (Siehe folgende Abbildung).



Hierarchie der Administrationsgruppen erstellen

Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Wählen Sie in der Hierarchie der Administrationsgruppen die Administrationsgruppe aus, welche die neue Administrationsgruppe enthalten soll.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.
4. Geben Sie im folgenden Fenster **Name der neuen Administrationsgruppe** den Namen der Gruppe ein, und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

In der Hierarchie der Administrationsgruppen erscheint eine neue Administrationsgruppe mit dem angegebenen Namen.

Das Programm ermöglicht, die Gruppenstruktur der Administrationsgruppen auf der Grundlage der Struktur von Active Directory oder der Struktur des Domänennetzwerks zu erstellen. Darüber hinaus können Sie die Gruppenstruktur auch aus einer Textdatei erstellen.

Um die Struktur der Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie auf die Schaltfläche **Importieren**.

   Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Anweisungen des Assistenten.

Geräte manuell zu einer Administrationsgruppe hinzufügen

Sie können Geräte automatisch in Administrationsgruppen verschieben, indem Sie Regeln zum Verschieben von Geräten erstellen oder manuell Geräte von einer Administrationsgruppe in eine andere verschieben oder Geräte einer ausgewählten Administrationsgruppe hinzufügen. Dieser Abschnitt beschreibt, wie Sie Geräte zu einer Administrationsgruppe manuell hinzufügen.

Um ein oder mehr Geräte zu einer ausgewählten Administrationsgruppe manuell hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie auf den Link **Aktueller Pfad:** `<aktueller Pfad>` über der Liste.
3. Wählen Sie im nächsten Fenster die Administrationsgruppe aus, zu der Sie die Geräte hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **Geräte hinzufügen**.

   Daraufhin wird der Assistent für das Verschieben von Geräten gestartet.
5. Erstellen Sie eine Liste mit Geräten, die Sie der Administrationsgruppe hinzufügen möchten.

   > Sie können nur Geräte hinzufügen, deren Informationen bereits durch Anschließen des Geräts oder nach einer Gerätesuche in die Administrationsserver-Datenbank eingetragen wurden.

   Wählen Sie aus, wie Sie Geräte zur Liste hinzufügen möchten:

   - Klicken Sie auf die Schaltfläche **Geräte hinzufügen**, und geben Sie die Geräte auf eine der folgenden Arten an:
     - Wählen Sie Geräte aus der Liste der vom Administrationsserver erkannten Geräte aus.
     - Geben Sie eine IP-Adresse oder einen IP-Bereich an.

       > Der IP-Bereich darf maximal 1.048.576 Adressen enthalten.

     - Geben Sie den NetBIOS-Namen oder DNS-Namen des Gerätes an.

       > Das Feld für die den Gerätenamen darf keine Leerzeichen sowie keins der folgenden verbotenen Zeichen enthalten: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

- Drücken Sie die Schaltfläche **Geräte aus Datei importieren**, um eine Liste von Geräten aus einer TXT-Datei zu importieren. Jede Adresse und jeder Name eines Gerätes müssen in einer separaten Zeile aufgeführt sein.

  Die Datei darf keine Leerzeichen sowie keins der folgenden verbotenen Zeichen enthalten: \ / * : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Zeigen Sie die Liste der Geräte an, die der Administrationsgruppe hinzugefügt werden sollen. Sie können die Liste bearbeiten, indem Sie Geräte hinzufügen oder entfernen.

7. Wenn Sie sichergestellt haben, dass die Liste korrekt ist, klicken Sie auf die Schaltfläche **Weiter**.

Der Assistent verarbeitet die Geräteliste und zeigt das Ergebnis an. Erfolgreich verarbeitete Geräte werden der Administrationsgruppe hinzugefügt und in der Geräteliste mit den Namen angezeigt, die der Administrationsserver bestimmt hat.

Manuelles Verschieben von Geräten oder Clustern in eine Administrationsgruppe

Sie können Geräte aus einer Administrationsgruppe in eine andere verschieben oder von der Gruppe nicht zugeordnete Geräte in eine Administrationsgruppe verschieben.

Sie können auch Cluster oder Server-Arrays von einer Administrationsgruppe in eine andere verschieben. Wenn Sie ein Cluster oder Server-Array in eine andere Gruppe verschieben, werden alle ihre Knoten mit verschoben, da ein Cluster und alle seine Knoten immer derselben Administrationsgruppe angehören. Wenn Sie auf der Registerkarte **Geräte** einen Cluster auswählen, wird die Schaltfläche **In Gruppe verschieben** inaktiv.

So verschieben Sie ein oder mehrere Geräte oder Cluster in eine ausgewählte Administrationsgruppe:

1. Öffnen Sie die Administrationsgruppe, aus welcher Sie die Geräte verschieben möchten. Führen Sie dazu eine der folgenden Aktionen aus:

   - Um eine Administrationsgruppe zu öffnen, gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**, klicken Sie auf den Pfad-Link im Feld **Aktueller Pfad** und wählen Sie im sich öffnenden linken Bereich eine Administrationsgruppe aus.

   - Um die Gruppe **Nicht zugeordnete Geräte** im Hauptmenü zu öffnen, wechseln Sie zu **Gerätesuche und Bereitstellung** → **Nicht zugeordnete Geräte**.

2. Wenn die Administrationsgruppe Cluster oder Server-Arrays enthält, wird der Abschnitt **Verwaltete Geräte** in zwei Registerkarten unterteilt – **Geräte** und **Cluster und Server-Arrays**. Öffnen Sie die Registerkarte für diese Art von Objekt, die Sie verschieben möchten.

3. Aktivieren Sie die Kontrollkästchen neben den Geräten oder Clustern, die Sie in eine andere Gruppe verschieben möchten.

4. Klicken Sie auf die Schaltfläche **In Gruppe verschieben**.

5. Aktivieren Sie in der Hierarchie der Verwaltungsgruppen das Kontrollkästchen neben der Administrationsgruppe, in welche Sie die ausgewählten Geräte oder Cluster verschieben möchten.

6. Klicken Sie auf die Schaltfläche **Verschieben**.

Die ausgewählten Geräte oder Cluster werden in die gewählte Administrationsgruppe verschoben.

Regeln für das Verschieben von Geräten erstellen

Sie können Verschiebungsregeln für Geräte einrichten, welche die Geräte automatisch den Administrationsgruppen zuzuordnen.

Um eine Verschiebungsregel zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verschiebungsregeln**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im nächsten Fenster auf der Registerkarte **Allgemein** die folgenden Informationen an:

   - **Regelname**

     Geben Sie einen Namen für die neue Regel ein.

     Wenn Sie eine Regel kopieren, erhält die neue Regel denselben Namen wie die ursprüngliche Regel, aber der Name wird um einen Index im Format () erweitert – z. B. (1).

   - **Administrationsgruppe**

     Wählen Sie die Administrationsgruppe aus, in welche die Geräte automatisch verschoben werden sollen.

   - **Aktive Regel**

     Wenn diese Option aktiviert ist, wird die Regel aktiviert und ab dem Speicherzeitpunkt berücksichtigt.

     Wenn diese Option deaktiviert ist, wird die Regel erstellt, aber nicht aktiviert. Sie wird erst berücksichtigt, sobald Sie diese Option aktivieren.

   - **Nur Geräte verschieben, die keiner Administrationsgruppe angehören**

     Wenn diese Option aktiviert ist, werden nur nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

     Wenn diese Option deaktiviert ist, werden Geräte, die bereits zu anderen Administrationsgruppen gehören, sowie nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

   - **Ausführung der Regel**

     Sie können eine der folgenden Varianten auswählen:

     - **Einmal pro Gerät ausführen**

       Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

     - **Einmal pro Gerät ausführen, danach bei jeder Neuinstallation des Administrationsagenten**

       Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt, und danach nur bei Neuinstallation des Administrationsagenten auf diesen Geräten.

     - **Regel fortlaufend ausführen**

       Die Regel wird gemäß einem Zeitplan angewendet, der automatisch vom Administrationsserver festgelegt wird (in der Regel alle paar Stunden).

4. Definieren Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium, nach dem die Geräte in eine Administrationsgruppe verschoben werden.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Verschiebungsregel wird erstellt. Sie wird in der Liste der Verschiebungsregeln angezeigt.

Je höher ihre Position in der Liste ist, desto höher ist die Priorität der Regel. Um die Priorität einer Verschiebungsregel zu erhöhen oder zu verringern, verschieben Sie die Regel mit der Maus in der Liste nach oben bzw. nach unten.

Wenn die Option **Regel fortlaufend ausführen** ausgewählt ist, wird die Verschiebungsregel unabhängig von der eingestellten Priorität angewendet. Diese Regeln werden gemäß dem Zeitplan angewendet, der automatisch vom Administrationsserver erstellt wird.

Wenn die Attribute des Geräts sofort einigen Regeln entsprechen, wird das Gerät in die Zielgruppe jener Regel verschoben, welche die höchste Priorität hat (in der Liste der Regeln weiter oben steht).

Regeln für das Verschieben von Geräten kopieren

Sie können Verschiebungsregeln kopieren, wenn Sie zum Beispiel mehrere identische Regeln für verschiedene Administrationszielgruppen haben möchten.

Um eine Verschiebungsregel zu kopieren, gehen Sie wie folgt vor:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verschiebungsregeln**.
   - Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Verschiebungsregeln**.

   Die Liste mit Verschiebungsregeln wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben der Regel, die Sie kopieren möchten.

3. Klicken Sie auf die Schaltfläche **Kopieren**.

4. Passen Sie im nächsten Fenster die folgenden Informationen auf der Registerkarte **Allgemein** an oder belassen Sie diese, wie sie sind, wenn Sie die Regel unverändert kopieren möchten:

   - **Regelname**

     Geben Sie einen Namen für die neue Regel ein.

     Wenn Sie eine Regel kopieren, erhält die neue Regel denselben Namen wie die ursprüngliche Regel, aber der Name wird um einen Index im Format () erweitert – z. B. (1).

   - **Administrationsgruppe**

     Wählen Sie die Administrationsgruppe aus, in welche die Geräte automatisch verschoben werden sollen.

- **Aktive Regel**

  Wenn diese Option aktiviert ist, wird die Regel aktiviert und ab dem Speicherzeitpunkt berücksichtigt.

  Wenn diese Option deaktiviert ist, wird die Regel erstellt, aber nicht aktiviert. Sie wird erst berücksichtigt, sobald Sie diese Option aktivieren.

- **Nur Geräte verschieben, die keiner Administrationsgruppe angehören**

  Wenn diese Option aktiviert ist, werden nur nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

  Wenn diese Option deaktiviert ist, werden Geräte, die bereits zu anderen Administrationsgruppen gehören, sowie nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

- **Ausführung der Regel**

  Sie können eine der folgenden Varianten auswählen:

  - **Einmal pro Gerät ausführen**

    Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

  - **Einmal pro Gerät ausführen, danach bei jeder Neuinstallation des Administrationsagenten**

    Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt, und danach nur bei Neuinstallation des Administrationsagenten auf diesen Geräten.

  - **Regel fortlaufend ausführen**

    Die Regel wird gemäß einem Zeitplan angewendet, der automatisch vom Administrationsserver festgelegt wird (in der Regel alle paar Stunden).

5. Definieren Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium für die Geräte, die automatisch verschoben werden sollen.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die neue Verschiebungsregel wird erstellt. Sie wird in der Liste der Verschiebungsregeln angezeigt.

Bedingungen für Verschiebungsregeln für Geräte

Wenn Sie eine Regel erstellen oder kopieren, um Client-Geräte in Administrationsgruppen zu verschieben, geben Sie auf der Registerkarte **Regelbedingungen** die Bedingungen zum Verschieben der Geräte an. Um festzulegen, welche Geräte verschoben werden sollen, können Sie die folgenden Kriterien verwenden:

- Den Client-Geräten zugewiesene Tags.
- Netzwerkparameter. Beispielsweise können Sie Geräte mit IP-Adressen aus einem bestimmten Bereich verschieben.
- Verwaltete Anwendungen, die auf Client-Geräten installiert sind, z. B. Administrationsagent oder Administrationsserver.
- Client-Geräte, die virtuelle Maschinen sind.
- Informationen über die Active Directory-Organisationseinheit (OU) mit den Client-Geräten.
- Informationen zu einem Cloud-Segment mit den Client-Geräten.

Nachfolgend finden Sie die Beschreibung, wie Sie diese Informationen in Verschiebungsregeln für Geräte angeben.

Wenn Sie in der Regel mehrere Bedingungen, werden alle mittels logischem UND-Operator verknüpft und alle Bedingungen gelten gleichzeitig. Wenn Sie gar keine Optionen auswählen oder einige Felder leer lassen, gelten diese Bedingungen nicht.

Registerkarte Tags

Auf dieser Registerkarte können Sie eine Verschiebungsregel für Geräte basierend auf Geräte-Tags anpassen, die den Beschreibungen der Client-Geräte zuvor hinzugefügt wurden. Wählen Sie dazu die erforderlichen Tags aus. Darüber hinaus können Sie die folgenden Optionen aktivieren:

- **Auf Geräte ohne angegebene Tags anwenden**

  Wenn diese Option aktiviert ist, werden alle Geräte mit den angegebenen Tags von einer Verschiebungsregel ausgeschlossen. Wenn diese Option deaktiviert ist, gilt die Verschiebungsregel für Geräte mit allen ausgewählten Tags.

  Diese Option ist standardmäßig deaktiviert.

- **Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft**

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregel für Client-Geräte mit mindestens einem der ausgewählten Tags. Wenn diese Option deaktiviert ist, gilt die Verschiebungsregel für Geräte mit allen ausgewählten Tags.

  Diese Option ist standardmäßig deaktiviert.

Registerkarte Netzwerk

Auf dieser Registerkarte können Sie die Netzwerkdaten von Geräten angeben, die eine Verschiebungsregel für Geräte berücksichtigt:

- **Gerätename im Windows-Netzwerk**

  Windows-Netzwerkname (NetBIOS-Name) des Geräts oder die IPv4- oder IPv6-Adresse.

- **Windows-Domäne**

  Eine Verschiebungsregel gilt für alle Geräte, die in der angegebenen Windows-Domäne enthalten sind.

- **DNS-Name des Geräts**

  Name der DNS-Domänen des Client-Geräts, das Sie verschieben möchten. Füllen Sie dieses Feld aus, wenn Ihr Netzwerk einen DNS-Server enthält.

  > Wenn für die Datenbank, die Sie für Kaspersky Security Center verwenden, die Unterscheidung zwischen Groß- und Kleinschreibung festgelegt ist, behalten Sie die Groß- und Kleinbuchstaben bei, wenn Sie einen DNS-Namen für das Gerät angeben. Andernfalls funktioniert die Verschiebungsregel für Geräte nicht.

- **DNS-Domäne**

  Eine Verschiebungsregel gilt für alle Geräte, die im angegebenen primären DNS-Suffix enthalten sind. Füllen Sie dieses Feld aus, wenn Ihr Netzwerk einen DNS-Server enthält.

- **IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

  Diese Option ist standardmäßig deaktiviert.

- **IP-Adresse für die Verbindung mit dem Administrationsserver**

  Wenn diese Option aktiviert ist, können Sie die IP-Adressen festlegen, über die Client-Geräte mit dem Administrationsserver verbunden werden. Geben Sie dazu den IP-Bereich an, der alle notwendigen IP-Adressen enthält.

  Diese Option ist standardmäßig deaktiviert.

- **Gerät befindet sich im IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie einen IP-Bereich auswählen, den Sie im Abschnitt **IP-Bereiche** zuvor hinzugefügt haben. Die betreffenden Geräte müssen im gewählten IP-Bereich enthalten sein.

  Diese Option ist standardmäßig deaktiviert.

- **Verbindungsprofil wurde geändert**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte mit einem geänderten Verbindungsprofil.
  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, deren Verbindungsprofile sich nicht geändert haben.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- **Verwaltung erfolgt durch anderen Administrationsserver**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte, die von anderen Administrationsservern verwaltet werden. Diese Server unterscheiden sich von dem Server, auf dem Sie die Verschiebungsregel für Geräte konfigurieren.
  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, die vom aktuellen Administrationsserver verwaltet werden.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

Registerkarte Programme

Auf dieser Registerkarte können Sie eine Regel zum Verschieben von Geräten basierend auf den verwalteten Anwendungen und Betriebssystemen konfigurieren, die auf Client-Geräten installiert sind:

- **Administrationsagent ist installiert**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte, auf denen der Administrationsagent installiert ist.
  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, auf denen der Administrationsagent nicht installiert ist.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- **Programme**

  Geben Sie an, welche verwalteten Anwendungen auf Client-Gerät installiert sein müssen, damit für diese Geräte eine Verschiebungsregel gilt. Sie können beispielsweise **Kaspersky Security Center 15.1 Administrationsagent** oder **Kaspersky Security Center 15.1 Administrationsserver** angeben.

  Wenn Sie keine verwaltete Anwendung auswählen, trifft die Bedingung nicht zu.

- **Version des Betriebssystems**

  Sie können Client-Geräte basierend auf deren Betriebssystemversionen auswählen. Geben Sie dazu Betriebssysteme an, die auf den Client-Geräten installiert sein müssen. Als Ergebnis gilt eine Verschiebungsregeln für die Client-Geräte mit den ausgewählten Betriebssystemen.

  Wenn Sie diese Option nicht aktivieren, trifft die Bedingung nicht zu. Die Option ist standardmäßig deaktiviert.

- **Bitzahl des Betriebssystems**

  Sie können Client-Geräte anhand der Bitanzahl des Betriebssystems auswählen. Im Block **Bitzahl des Betriebssystems** können Sie einen der folgenden Werte auswählen:

  - **Unbekannt**
  - **x86**
  - **AMD64**
  - **IA64**

  So überprüfen Sie die Bitanzahl des Betriebssystems der Client-Geräte:

  1. Gehen Sie im Hauptmenü zum Abschnitt **Assets (Geräte)** → **Verwaltete Geräte**.
  2. Klicken Sie auf die Schaltfläche **Spalteneinstellungen** (⚙) auf der rechten Seite.
  3. Aktivieren Sie die Option **Bitzahl des Betriebssystems** und klicken Sie anschließend auf die Schaltfläche **Speichern**.

     Danach wird die Bitanzahl des Betriebssystems für jedes verwaltete Gerät angezeigt.

- **Service Pack-Version des Betriebssystems**

  In diesem Feld können Sie die Service Pack-Version (im Format *X.Y*) des Betriebssystems angeben, die bestimmt, wie die Verschiebungsregel auf das Gerät angewendet wird. Standardmäßig ist keine Version angegeben.

- **Benutzerzertifikat**

  Wählen Sie eine der folgenden Werte aus:

  - **Installiert**. Eine Verschiebungsregel gilt nur für mobile Geräte mit einem Mobilgerät-Zertifikat.
  - **Nicht installiert**. Die Verschiebungsregel gilt nur für mobile Geräte ohne Mobilgerät-Zertifikat.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- **Build-Version des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Verschiebungsregel für Geräte für alle Versionsnummern mit Ausnahme der angegebenen anpassen.

- **Releasenummer des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-Nummer haben muss. Sie können auch eine Verschiebungsregel für Geräte für allen Versionsnummern mit Ausnahme der angegebenen anpassen.

Registerkarte Virtuelle Maschinen

Auf dieser Registerkarte können Sie die Verschiebungsregel für Geräte anpassen, je nachdem, ob die Client-Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- **Ist eine virtuelle Maschine**

  In der Dropdown-Liste können Sie einen der folgenden Werte auswählen:

  - **N/A**. Die Bedingung trifft nicht zu.
  - **Nein**. Geräte verschieben, die keine virtuellen Maschinen sind.
  - **Ja**. Geräte verschieben, die virtuellen Maschinen sind.

- **Typ der virtuellen Maschine**

- **Gehört zur Virtual Desktop Infrastructure (VDI)**

  In der Dropdown-Liste können Sie einen der folgenden Werte auswählen:

  - **N/A**. Die Bedingung trifft nicht zu.
  - **Nein**. Geräte verschieben, die keine Teil einer VDI sind.
  - **Ja**. Geräte verschieben, die Teil einer VDI sind.

Registerkarte Domänencontroller

Auf dieser Registerkarte können Sie angeben, dass Geräte verschoben werden sollen, die in der Domänen-Organisationseinheit enthalten sind. Sie können auch Geräte aus allen untergeordneten Organisationseinheiten der angegebenen Domänen-Organisationseinheit verschieben:

- **Das Gerät befindet sich in folgender Organisationseinheit**

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregel für die Geräte aus der Domänen-Organisationseinheit, die in der Liste unter der Option angegeben ist.

  Diese Option ist standardmäßig deaktiviert.

- **Untergeordnete Organisationseinheiten einschließen**

  Wenn die Option aktiviert ist, werden die Geräte aus allen untergeordneten Organisationseinheiten der angegebenen Domänen-Organisationseinheit aufgenommen.

  Diese Option ist standardmäßig deaktiviert.

- **Geräte aus untergeordneten Organisationseinheiten in entsprechende Untergruppen verschieben**
- **Untergruppen erstellen, die Containern von neu erkannten Geräten entsprechen**
- **Untergruppen löschen, die in der Domäne fehlen**
- **Das Gerät ist Mitglied der folgenden Domänensicherheitsgruppe**

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregel für die Geräte aus der Domänensicherheitsgruppe, die in der Liste unter der Option angegeben ist.

  Diese Option ist standardmäßig deaktiviert.

Registerkarte Cloud-Segmente

Auf dieser Registerkarte können Sie angeben, dass Geräte verschoben werden sollen, die zu bestimmten Cloud-Segmenten gehören:

- **Gerät befindet sich in einem Cloud-Segment**

  Wenn Sie diese Option auswählen, gilt eine Verschiebungsregeln für Geräte für die Client-Geräte, die zu einem Cloud-Segment gehören. In der Liste unter der Option können Sie das gewünschte Cloud-Segment bis hin zu einem Subnetz auswählen.

  Die Option ist standardmäßig deaktiviert.

- **Untergeordnete Objekte einschließen**

  Wenn Sie diese Option auswählen, gilt eine Verschiebungsregeln für Geräte nicht nur für das ausgewählte Cloud-Segment, sondern auch für die untergeordneten Objekte dieses Segments.

  Die Option ist standardmäßig deaktiviert.

- **Geräte aus untergeordneten Objekten in entsprechende Gruppen verschieben**
- **Untergruppen erstellen, die Containern von neu erkannten Geräten entsprechen**
- **Untergruppen ohne Entsprechungen in Cloud-Segmenten löschen**

- **Gerät mittels API erkannt**

  In der Dropdown-Liste können Sie wählen, ob das Gerät über API gefunden werden soll:

  - **AWS**. Das Gerät wird mithilfe der AWS-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von AWS.
  - **Azure**. Das Gerät wird mithilfe der Azure-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Azure.
  - **Google Cloud.** Das Gerät wird mithilfe der Google-API gefunden, d. h. es befindet sich definitiv in der Cloud-Umgebung von Google.
  - **Nein**. Das Gerät wird nicht mithilfe der AWS-, Azure- oder Google-API gefunden. Das heißt, es befindet sich entweder außerhalb der Cloud-Umgebung oder es befindet sich in der Cloud-Umgebung, ist aber für die Suche mithilfe API nicht auffindbar.
  - **Kein Wert**. Diese Bedingung trifft nicht zu.

Über Cluster und Server-Arrays

Kaspersky Security Center unterstützt Cluster-Technologie. Sobald der Administrationsserver vom Administrationsagenten die Information erhält, dass ein auf einem Client-Gerät installiertes Programm zum Server-Array gehört, wird das betreffende Client-Gerät als Knoten in dem Cluster eingebunden.

Wenn eine Administrationsgruppe Cluster oder Server-Arrays enthält, zeigt die Seite **Verwaltete Geräte** zwei Registerkarten an – eine für einzelne Geräte und eine für Cluster und Server-Arrays. Nachdem die verwalteten Geräte als Cluster-Knoten erkannt wurden, wird der Cluster als einzelnes Objekt zur Registerkarte **Cluster und Server-Arrays** hinzugefügt.

Die Knoten des Clusters oder Server-Arrays werden zusammen mit anderen verwalteten Geräten auf der Registerkarte **Geräte** angezeigt. Sie können für die Knoten wie für andere Geräte Eigenschaften anzeigen und weitere Operationen durchführen, aber Sie können einen Cluster-Knoten nicht löschen oder ihn getrennt von seinem Cluster in eine andere Administrationsgruppe verschieben. Sie können nur einen ganzen Cluster löschen oder verschieben.

Die folgenden Vorgänge können Sie mit Clustern oder Server-Arrays ausführen:

- Eigenschaften anzeigen
- Das Cluster oder Server-Array in eine andere Administrationsgruppe verschieben

  Wenn Sie ein Cluster oder Server-Array in eine andere Gruppe verschieben, werden alle ihre Knoten mit verschoben, da ein Cluster und alle seine Knoten immer derselben Administrationsgruppe angehören.

- Löschen

  Es ist nur dann sinnvoll, ein Cluster oder ein Server-Array zu löschen, wenn das Cluster oder Server-Array nicht mehr im Netzwerk der Organisation existiert. Wenn ein Cluster noch in Ihrem Netzwerk sichtbar ist und der Administrationsagent und die Kaspersky-Sicherheitsanwendung noch auf den Cluster-Knoten installiert sind, fügt Kaspersky Security Center das gelöschte Cluster und seine Knoten automatisch wieder zur Liste der verwalteten Geräte hinzu.

Eigenschaften eines Cluster- oder Server-Arrays

So zeigen Sie die Einstellungen eines Clusters oder Server-Arrays an:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte** → **Cluster und Server-Arrays**.

   Die Liste der Cluster und Server-Arrays wird angezeigt.

2. Klicken Sie auf den Namen des erforderlichen Clusters oder Server-Arrays.

Das Eigenschaftenfenster des gewählten Clusters oder Server-Arrays wird geöffnet.

Allgemein

Der Abschnitt **Allgemein** zeigt allgemeine Informationen zu dem Cluster oder Server-Array an. Die Informationen beruhen auf Daten, die bei der letzten Synchronisierung der Cluster-Knoten mit dem Administrationsserver empfangen wurden:

- **Name**
- **Beschreibung**
- **Windows-Domäne**

  Windows-Domäne oder -Arbeitsgruppe, die das Cluster oder Server-Array enthält.

- **NetBIOS-Name**

  Windows-Netzwerkname des Clusters oder Server-Arrays.

- **DNS-Name**

  Name der DNS-Domäne des Clusters oder Server-Arrays.

Aufgaben

In der Registerkarte **Aufgaben** können Sie die dem Cluster oder Server-Array zugewiesenen Aufgaben verwalten: Liste der vorhandenen Aufgaben anzeigen, neue Aufgaben erstellen, Aufgaben entfernen, starten und beenden, Aufgabeneinstellungen ändern und die Ergebnisse der Aufgabenausführung anzeigen. Die aufgeführten Aufgaben beziehen sich auf die Kaspersky-Sicherheitsanwendung, die auf den Cluster-Knoten installiert ist.
Kaspersky Security Center bezieht die Aufgabenliste und die Details zum Aufgabenstatus von den Cluster-Knoten. Wenn keine Verbindung hergestellt ist, wird der Status nicht angezeigt.

Knoten

Diese Registerkarte zeigt eine Liste der Knoten an, die im Cluster oder Server-Array enthalten sind. Sie können auf den Namen eines Knotens klicken, um das Fenster mit den Geräteeigenschaften anzuzeigen.

Kaspersky-Anwendung

Das Eigenschaftenfenster kann auch zusätzliche Registerkarten mit Informationen und Einstellungen bezüglich der auf den Cluster-Knoten installierten Kaspersky-Sicherheitsanwendung enthalten.

Maßnahmen anzeigen und konfigurieren, wenn Geräte als inaktiv angezeigt werden

Wenn Client-Geräte innerhalb einer Gruppe inaktiv sind, können Sie Benachrichtigungen darüber erhalten. Sie können solche Geräte auch automatisch löschen.

Um die Aktionen bei inaktiven Geräten innerhalb einer Gruppe anzuzeigen oder anzupassen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie auf den Namen der gewünschten Administrationsgruppe.

   Das Eigenschaftenfenster der übergeordneten Administrationsgruppe wird geöffnet.
3. Gehen Sie im Eigenschaftenfenster zur Registerkarte **Einstellungen**.
4. Aktivieren oder deaktivieren Sie im Abschnitt **Vererbung** die folgenden Optionen:

   - **Aus übergeordneter Gruppe erben**

     Die Einstellungen in diesem Abschnitt werden von der übergeordneten Gruppe geerbt, in der das Client-Gerät enthalten ist. Wenn diese Option aktiviert ist, sind die Einstellungen unter **Geräteaktivität im Netzwerk** für alle Änderungen gesperrt.

     Diese Option ist nur verfügbar, wenn die Administrationsgruppe über eine übergeordnete Gruppe verfügt.

     Diese Option ist standardmäßig aktiviert.

   - **Vererbung der Einstellungen an untergeordnete Gruppen erzwingen**

     Die Einstellungswerte werden an untergeordnete Gruppen verteilt, aber in den Eigenschaften der untergeordneten Gruppen sind diese Einstellungen gesperrt.

     Diese Option ist standardmäßig deaktiviert.
5. Aktivieren oder deaktivieren Sie im Abschnitt **Geräteaktivität** die folgenden Optionen:

   - **Administrator benachrichtigen, wenn Gerät inaktiv seit (Tagen)**

     Wenn diese Option aktiviert ist, erhält der Administrator Benachrichtigungen über inaktive Geräte. Sie können das Zeitintervall angeben, nach dem das Ereignis **Gerät zu lange inaktiv im Netzwerk** erstellt wird. Standardmäßig beträgt das Zeitintervall 7 Tage.

     Diese Option ist standardmäßig aktiviert.

   - **Gerät aus Gruppe entfernen, wenn Gerät inaktiv seit (Tagen)**

     Wenn diese Option aktiviert ist, können Sie das Zeitintervall festlegen, nach dem das Geräte automatisch aus der Gruppe gelöscht wird. Standardmäßig beträgt das Zeitintervall 60 Tage.

Diese Option ist standardmäßig aktiviert.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Ihre Änderungen werden gespeichert und übernommen.

Über die Varianten für den Gerätestatus

Kaspersky Security Center weist jedem verwalteten Gerät einen Status zu. Der jeweilige Status hängt davon ab, ob die vom Benutzer definierten Bedingungen erfüllt sind. Wenn Kaspersky Security Center einem Gerät einen Status zuweist, wird in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). Beispiel: Wenn einem verwalteten Gerät der Status *Kritisch* zugewiesen wurde, da die Bedingung *Die Datenbanken sind veraltet* erfüllt ist und für das Gerät später das Sichtbarkeits-Flag gesetzt wurde, erhält das Gerät den Status *OK*. Wenn Kaspersky Security Center ein Gerät innerhalb von zwei Stunden nicht im Netzwerk findet, wird das Sichtbarkeits-Flag des Gerätes auf *Nicht sichtbar* gesetzt.

Es gibt folgende Statusvarianten:

- *Kritisch* oder *Kritisch / Sichtbar*
- *Warnung* oder *Warnung / Sichtbar*
- *OK* oder *OK / Sichtbar*

Die folgende Tabelle enthält die erforderlichen Standardbedingungen, nach denen einem Gerät der Status *Kritisch* oder *Warnung* zugewiesen wird, sowie alle möglichen Werte.

Bedingungen für das Zuweisen der Status an das Gerät

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Es wurde keine Sicherheitsanwendung installiert	Auf dem Gerät ist der Administrationsagent installiert, aber es wurde keine Sicherheitsanwendung installiert.	• Umschalter aktiviert. • Umschalter deaktiviert.
Zu viele Viren gefunden	Auf dem Gerät wurden als Ergebnis der Ausführung einer Aufgabe zur Virensuche (beispielsweise der Aufgabe zur *Schadsoftware-Untersuchung*) mehrere Viren gefunden, und die Anzahl der gefundenen Viren übersteigt den angegebenen Wert.	Über 0.
Die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die der Administrator festgelegt hat	Das Gerät ist im Netzwerk sichtbar, aber die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die vom Administrator (in der Bedingung) für den Gerätestatus eingestellt wurde.	• Beendet. • Angehalten. • Wird ausgeführt.
Die letzte Schadsoftware-Untersuchung liegt lange zurück	Das Gerät ist im Netzwerk sichtbar und es wurde eine Sicherheitsanwendung auf dem Gerät installiert, aber es wurde weder die Aufgabe zur *Schadsoftware-Untersuchung*, noch die Aufgabe zur lokalen Untersuchung innerhalb des angegebenen Zeitintervalls ausgeführt. Die Bedingung gilt nur für Geräte, die vor mehr als sieben Tagen zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.
Die Datenbanken sind veraltet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung wurde auf dem Gerät installiert, aber die Antiviren-Datenbanken wurden auf diesem Gerät nicht innerhalb des angegebenen Zeitintervalls aktualisiert. Die Bedingung gilt nur für Geräte, die vor mehr als einem Tag zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.
Die letzte Verbindung liegt lange zurück	Der Administrationsagent ist auf dem Gerät installiert, es wurde allerdings nicht innerhalb des angegebenen Zeitintervalls mit dem Administrationsserver verbunden, da es deaktiviert ist.	Über 1 Tag.
Aktive Bedrohungen werden erkannt	Die Anzahl der unbearbeiteten Objekte im Ordner **Aktive Bedrohungen** übersteigt den angegebenen Wert.	Über 0 Elemente.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Neustart erforderlich	Das Gerät ist im Netzwerk sichtbar, aber eine Anwendung erfordert aufgrund einer der angegeben Bedingungen einen Neustart des Gerätes, der nicht innerhalb des festgelegten Zeitraums ausgeführt wurde.	Über 0 Minuten.
Es sind inkompatible Anwendungen installiert	Das Gerät ist im Netzwerk sichtbar, aber infolge der Inventarisierung der Software durch den Administrationsagenten wurden auf dem Gerät inkompatible Anwendungen gefunden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden Schwachstellen in Programmen erkannt	Das Gerät ist im Netzwerk sichtbar und der Administrationsagent ist auf dem Gerät installiert, aber die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* hat in den Programmen auf dem Gerät Schwachstellen mit der angegebenen Signifikanz gefunden.	• Kritisch. • Hoch. • Normal. • Ignorieren, wenn die Schwachstelle nicht geschlossen werden kann. • Ignorieren, wenn das Update für die Installation bestimmt wurde.
Lizenz abgelaufen	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz ist abgelaufen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Die Lizenz läuft bald ab	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz auf dem Gerät läuft in weniger als der angegebenen Anzahl an Tagen ab.	Weniger als 0 Tage.
Die letzte Suche nach Windows-Updates liegt lange zurück	Das Gerät ist im Netzwerk sichtbar, aber die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* wurde nicht innerhalb des angegebenen Zeitintervalls ausgeführt.	Über 1 Tag.
Ungültiger Verschlüsselungsstatus	Der Administrationsagent ist auf dem Gerät installiert, aber das Ergebnis der Verschlüsselung des Geräts entspricht dem angegebenen Wert.	• Entspricht nicht der Richtlinie aufgrund der Ablehnung durch den Benutzer (nur für externe Geräte). • Entspricht nicht der Richtlinie wegen eines Fehlers. • Bei der Übernahme der Richtlinie – Neustart erforderlich. • Es wurde keine Verschlüsselungsrichtlinie festgelegt. • Nicht unterstützt. • Bei der Übernahme der Richtlinie.
Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie	Die Einstellungen des mobilen Geräts unterscheiden sich von den in der Richtlinie von Kaspersky Endpoint Security für Android festgelegten Einstellungen beim Ausführen der Untersuchung der Übereinstimmungsregeln.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden unbearbeitete Sicherheitsprobleme erkannt	Auf dem Gerät sind unbearbeitete Sicherheitsvorfälle vorhanden. Sicherheitsvorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten verwalteten Kaspersky-Anwendungen als auch manuell durch den Administrator erstellt werden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Gerätestatus wird vom Programm bestimmt	Der Gerätestatus wird von der verwalteten Anwendung bestimmt. Verwaltete Geräte können einen Status besitzen, der von den verwalteten Anwendungen unabhängig von den Einstellungen von Kaspersky Security Center bestimmt wird. Wenn der Status zu einem der Werte zurückkehrt, die durch Kaspersky Security Center bestimmt werden, weist der Administrationsserver einem verwalteten Gerät den kritischsten Status zu, der von der verwalteten Anwendung zurückgegeben und vom Administrationsserver zugewiesen wurde. Statuswerte, die von verwalteten Anwendungen bestimmt werden, besitzen Beschreibungen, die ebenfalls von den verwalteten Anwendungen stammen. Sie können diese Beschreibungen in der Liste der verwalteten Geräte in der Spalte **Statusbeschreibung**.	• Umschalter ist deaktiviert. • Umschalter ist aktiviert.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Kein Platz auf dem Datenträger des Geräts	Der freie Speicherplatz auf dem Datenträger ist kleiner als der angegebene Wert oder das Gerät konnte nicht mit dem Administrationsserver synchronisiert werden. Der Status *Kritisch* oder *Warnung* wird in den Status *OK* geändert, wenn das Gerät erfolgreich mit dem Administrationsserver synchronisiert wird und der freie Speicherplatz auf dem Gerät dem angegebenen Wert entspricht oder diesen überschreitet.	Über 0 MB.
Das Gerät wird nicht mehr verwaltet	Bei der Gerätesuche ist das Gerät im Netzwerk sichtbar, aber es sind mehr als drei Synchronisierungsversuche mit dem Administrationsserver fehlgeschlagen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Der Schutz ist deaktiviert	Das Gerät ist im Netzwerk sichtbar, aber die Sicherheitsanwendung auf dem Gerät ist länger deaktiviert, als im Zeitintervall angegeben. In diesem Fall lautet der Status der Sicherheitsanwendung *Angehalten* oder *Fehler* und unterscheidet sich von den folgenden Statuswerten *Wird gestartet*, *Wird ausgeführt* oder *Wird angehalten*.	Über 0 Minuten.
Die Sicherheitsanwendung wurde nicht gestartet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung ist auf dem Gerät installiert, wurde aber nicht gestartet.	• Umschalter deaktiviert. • Umschalter aktiviert.

Kaspersky Security Center ermöglicht eine Konfiguration der automatischen Umschaltung des Status von Geräten in der Administrationsgruppe bei Erfüllung der angegebenen Bedingungen. Bei Erfüllung der festgelegten Bedingungen wird dem Client-Gerät einer der folgenden Statuswerte verliehen: *Kritisch* oder *Warnung*. Sind die festgelegten Bedingungen nicht erfüllt, so erhält das Client-Gerät den Status *OK*.

Verschiedenen Werten einer einzelnen Bedingung können verschiedene Statusvarianten entsprechen. Beispiele: Wenn die Bedingung **Die Datenbanken sind veraltet** den Wert **Über 3 Tage** besitzt, erhält das Client-Gerät standardmäßig den Status *Warnung*; für den Wert **Über 7 Tage** wird der Status *Kritisch* zugewiesen.

Wenn Sie Kaspersky Security Center von der vorhergehenden Version aktualisieren, ändern sich nicht die Werte zum Zuweisen des Status *Kritisch* oder *Warnung* für die Bedingung **Die Datenbanken sind veraltet**.

Wechsel der Statuswerte von Geräten konfigurieren

Sie können die Bedingungen ändern, um einem Gerät den Status *Kritisch* oder *Warnung* zuzuweisen.

Um die Änderungen des Gerätestatus auf Kritisch zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Kritisch** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Kritisch" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Kritisch*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.

8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.

9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Warnung** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Warnung" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Warnung*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.

9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Remotedesktopverbindung mit dem Client-Gerät herstellen

Der Administrator kann Remotezugriff auf den Desktop des Client-Geräts mithilfe des Administrationsagenten bekommen, der auf dem Client-Gerät installiert wurde. Die Remoteverbindung mit dem Client-Gerät mithilfe des Administrationsagenten ist sogar dann möglich, wenn die TCP- und UDP-Ports des Client-Geräts geschlossen sind.

Nach der Verbindung mit dem Gerät bekommt der Administrator vollständigen Zugriff auf die Informationen dieses Geräts und kann die auf diesem Gerät installierten Programme verwalten.

Die Remoteverbindung muss in den Betriebssystemeinstellungen des verwalteten Zielgeräts erlaubt sein. In Windows 10 heißt diese Option beispielsweise **Remoteverbindungen mit diesem Computer zulassen** (diese Option finden Sie unter **Systemsteuerung** → **Alle Systemsteuerungselemente** → **System und Sicherheit** → **Remoteeinstellungen**). Wenn Sie über eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" verfügen, können Sie das Aktivieren dieser Option erzwingen, wenn Sie eine Verbindung zu einem verwalteten Gerät herstellen. Wenn Sie nicht über diese Lizenz verfügen, aktivieren Sie diese Option lokal auf dem verwalteten Zielgerät. Es ist keine Remoteverbindung möglich, wenn diese Option deaktiviert ist.

Um eine Remoteverbindung mit einem Gerät herzustellen, benötigen Sie zwei Dienstprogramme:

- Das Kaspersky-Dienstprogramm "klsctunnel". Das Dienstprogramm muss sich auf Administrator-Arbeitsplatz befinden. Mit diesem Dienstprogramm können Sie die Verbindung zwischen einem Client-Gerät und dem Administrationsserver tunneln.

  Kaspersky Security Center erlaubt das Tunneln der TCP-Verbindungen von der Verwaltungskonsole über den Administrationsserver und weiter über den Administrationsagenten zum angegebene Port auf dem verwalteten Gerät. Das Tunneln wird für den Fall, dass eine direkte Verbindung des Geräts mit der Verwaltungskonsole unmöglich ist, für die Verbindung des Client-Programms, welches sich auf dem Gerät mit der installierten Verwaltungskonsole befindet, zum TCP-Port des verwalteten Gerät verwendet.

  Es ist erforderlich, die Verbindung eines Remote-Client-Geräts mit dem Administrationsserver zu tunneln, wenn der Port für die Verbindung mit dem Administrationsserver auf dem Gerät nicht verfügbar ist. Der Port auf dem Gerät kann in folgenden Fällen nicht verfügbar sein:

  - Das Remote-Gerät ist mit einem lokalen Netzwerk verbunden, in dem das NAT-Verfahren verwendet wird.
  - Das Remote-Gerät gehört zum lokalen Netzwerk des Administrationsservers, sein Port wird jedoch von der Firewall geschlossen.

- Die Standard-Komponente von Microsoft Windows "Remotedesktopverbindung". Die Remotedesktopverbindung erfolgt mithilfe des Windows-Standardtools mstsc.exe gemäß den Einstellungen des Dienstprogramms.

  Die Verbindung zu einer bestehenden Sitzung des Remotedesktops des Benutzers wird ohne Benachrichtigung des Benutzers hergestellt. Nachdem sich der Administrator mit der Sitzung verbunden hat, wird der Benutzer des Client-Geräts ohne vorherige Benachrichtigung von der Sitzung abgemeldet.

Um eine Verbindung mit Desktop eines Client-Geräts herstellen:

1. Wählen Sie in der MMC-basierten Verwaltungskonsole des Administrationsservers den Punkt **Eigenschaften** aus.
2. Wechseln Sie im folgenden Eigenschaftenfenster des Administrationsservers zu **Verbindungseinstellungen des Administrationsservers → Verbindungsports**.
3. Stellen Sie sicher, dass der Option **RDP-Port der Kaspersky Security Center Web Console öffnen** aktiviert ist.
4. Wechseln Sie in der Kaspersky Security Center Web Console zu **Assets (Geräte) → Verwaltete Geräte**.
5. Klicken Sie im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte auf den Pfad-Link.
6. Wählen Sie im angezeigten linken Bereich die Administrationsgruppe mit dem Gerät aus, auf das Sie Zugriff erhalten möchten.
7. Aktivieren Sie das Kontrollkästchen neben dem Namen des Geräts, für das Sie Zugriff benötigen.
8. Klicken Sie auf die Schaltfläche **Remotedesktopverbindung herstellen**.

   Das Fenster "Remotedesktop (nur Windows)" wird geöffnet.

9. Aktivieren Sie die Option **Remotedesktopverbindung auf verwaltetem Gerät zulassen**. In diesem Fall wird die Verbindung auch dann hergestellt, wenn Remoteverbindungen derzeit in den Betriebssystemeinstellungen auf dem verwalteten Gerät verboten sind.

   Diese Option ist nur verfügbar, wenn Sie über eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" verfügen.

10. Klicken Sie auf die Schaltfläche **Herunterladen**, um das Dienstprogramm "klsctunnel" herunterzuladen.

11. Klicken Sie auf die Schaltfläche **In die Zwischenablage kopieren**, um den Text aus dem Textfeld zu kopieren. Dieser Text ist ein Binary Large Object (BLOB), welches die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlichen Einstellungen enthält.

    Ein BLOB ist 3 Minuten gültig. Wenn der BLOB abgelaufen ist, öffnen Sie das Fenster "Remotedesktop (nur Windows)" erneut, um einen neuen BLOB zu generieren.

12. Führen Sie das Dienstprogramm "klsctunnel" aus.

    Das Fenster des Dienstprogramms wird geöffnet.

13. Fügen Sie den kopierten Text in das Textfeld ein.

14. Wenn Sie einen Proxyserver verwenden, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie dann die Verbindungseinstellungen für den Proxyserver ein.

15. Klicken Sie auf die Schaltfläche **Port öffnen**.

    Das Anmeldefenster für die Remotedesktopverbindung wird geöffnet.

16. Geben Sie die Anmeldeinformationen des Kontos an, mit dem Sie derzeit bei Kaspersky Security Center Web Console angemeldet sind.

17. Klicken Sie auf die Schaltfläche **Verbinden**.

Nach der Verbindung mit dem Client-Gerät ist der Desktop des Client-Geräts im Microsoft Windows-Fenster für Remoteverbindung verfügbar.

Verbindung mit den Client-Geräten über die Windows Desktopfreigabe herstellen

Der Administrator kann Remotezugriff auf den Desktop des Client-Geräts mithilfe des Administrationsagenten bekommen, der auf dem Client-Gerät installiert wurde. Die Remoteverbindung mit dem Client-Gerät mithilfe des Administrationsagenten ist sogar dann möglich, wenn die TCP- und UDP-Ports des Client-Geräts geschlossen sind.

Der Administrator kann eine Verbindung mit der vorhandenen Sitzung auf dem Client-Gerät herstellen, ohne dass der Benutzer dieser Sitzung getrennt wird. In diesem Fall haben der Administrator und der Benutzer der Sitzung auf dem Gerät einen gemeinsamen Zugriff auf den Desktop.

Um eine Remoteverbindung mit einem Gerät herzustellen, benötigen Sie zwei Dienstprogramme:

- Das Kaspersky-Dienstprogramm "klsctunnel". Das Dienstprogramm muss sich auf Administrator-Arbeitsplatz befinden. Mit diesem Dienstprogramm können Sie die Verbindung zwischen einem Client-Gerät und dem Administrationsserver tunneln.

  Kaspersky Security Center erlaubt das Tunneln der TCP-Verbindungen von der Verwaltungskonsole über den Administrationsserver und weiter über den Administrationsagenten zum angegebene Port auf dem verwalteten Gerät. Das Tunneln wird für den Fall, dass eine direkte Verbindung des Geräts mit der Verwaltungskonsole unmöglich ist, für die Verbindung des Client-Programms, welches sich auf dem Gerät mit der installierten Verwaltungskonsole befindet, zum TCP-Port des verwalteten Gerät verwendet.

  Es ist erforderlich, die Verbindung eines Remote-Client-Geräts mit dem Administrationsserver zu tunneln, wenn der Port für die Verbindung mit dem Administrationsserver auf dem Gerät nicht verfügbar ist. Der Port auf dem Gerät kann in folgenden Fällen nicht verfügbar sein:

  - Das Remote-Gerät ist mit einem lokalen Netzwerk verbunden, in dem das NAT-Verfahren verwendet wird.
  - Das Remote-Gerät gehört zum lokalen Netzwerk des Administrationsservers, sein Port wird jedoch von der Firewall geschlossen.

- Windows Desktopfreigabe. Bei der Verbindung mit einer vorhandenen Remotedesktop-Sitzung empfängt der Benutzer der Sitzung auf dem Gerät eine Anfrage zum Herstellen der Verbindung vom Administrator. Die Informationen über die Aktivitäten auf dem Remote-Gerät und deren Ergebnisse werden in den Kaspersky Security Center-Berichten nicht gespeichert.

  Der Administrator kann ein Audit der Aktionen auf dem Remote-Client-Gerät konfigurieren. Während des Audits werden Informationen über die Dateien auf dem Client-Gerät gesammelt, die vom Administrator geöffnet bzw. geändert werden.

Um sich mittels Windows Desktopfreigabe mit dem Desktop eines Client-Geräts zu verbinden, müssen die folgenden Voraussetzungen erfüllt sein:

- Auf dem Administrator-Arbeitsplatz ist Microsoft Windows Vista oder höher installiert. Für die Herstellung einer Verbindung mithilfe der Windows Desktopfreigabe gibt es keine Einschränkungen hinsichtlich des Betriebssystemtyps des Geräts, auf dem der Administrationsserver installiert ist.

  Um zu prüfen, ob die Funktion für die Windows Desktopfreigabe in Ihrer Windows-Edition enthalten ist, stellen Sie sicher, dass der Schlüssel "CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F}" in der Windows-Registry enthalten ist.

- Microsoft Windows Vista oder höher ist auf dem Client-Gerät installiert.

- Kaspersky Security Center nutzt eine Lizenz für Schwachstellen- und Patch-Management.

Um eine Verbindung mit dem Client-Gerät-Desktop über Windows Desktopfreigabe herzustellen, gehen Sie wie folgt vor:

1. Wählen Sie in der MMC-basierten Verwaltungskonsole des Administrationsservers den Punkt **Eigenschaften** aus.
2. Wechseln Sie im folgenden Eigenschaftenfenster des Administrationsservers zu **Verbindungseinstellungen des Administrationsservers** → **Verbindungsports**.
3. Stellen Sie sicher, dass der Option **RDP-Port der Kaspersky Security Center Web Console öffnen** aktiviert ist.
4. Wechseln Sie in der Kaspersky Security Center Web Console zu **Assets (Geräte)** → **Verwaltete Geräte**.

5. Klicken Sie im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte auf den Pfad-Link.
6. Wählen Sie im angezeigten linken Bereich die Administrationsgruppe mit dem Gerät aus, auf das Sie Zugriff erhalten möchten.
7. Aktivieren Sie das Kontrollkästchen neben dem Namen des Geräts, für das Sie Zugriff benötigen.
8. Klicken Sie auf die Schaltfläche **Windows Desktopfreigabe**.

   Der Assistent für die Windows Desktopfreigabe öffnet sich.
9. Klicken Sie auf die Schaltfläche **Herunterladen** um das Programm "klsctunnel" herunterzuladen und warten Sie, bis der Prozess abgeschlossen ist.

   Wenn Sie das "klsctunnel"-Dienstprogramm bereits besitzen, überspringen Sie diesen Schritt.
10. Klicken Sie auf die Schaltfläche **Weiter**.
11. Wählen Sie die Sitzung auf dem Gerät, mit dem Sie sich verbinden möchten, und klicken Sie auf **Weiter**.
12. Auf dem Zielgerät öffnet sich ein Dialogfenster und der Nutzer muss die Sitzung für die Desktopfreigabe zulassen. Andernfalls ist die Sitzung nicht möglich.

    Nachdem der Gerätenutzer die Sitzung für die Desktopfreigabe zugelassen hat, öffnet sich die nächste Seite des Assistenten.
13. Klicken Sie auf die Schaltfläche **In die Zwischenablage kopieren**, um den Text aus dem Textfeld zu kopieren. Dieser Text ist ein Binary Large Object (BLOB), welches die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlichen Einstellungen enthält.

    > Ein BLOB ist 3 Minuten gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.
14. Führen Sie das Dienstprogramm "klsctunnel" aus.

    Das Fenster des Dienstprogramms wird geöffnet.
15. Fügen Sie den kopierten Text in das Textfeld ein.
16. Wenn Sie einen Proxyserver verwenden, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie dann die Verbindungseinstellungen für den Proxyserver ein.
17. Klicken Sie auf die Schaltfläche **Port öffnen**.

Die Desktopfreigabe startet in einem neuen Fenster. Wenn Sie das Gerät steuern möchten, klicken Sie das Menü-Symbol () in der linken oberen Ecke des Fensters und wählen Sie anschließend **Interaktiver Modus** aus.

Geräteauswahlen

Geräteauswahlen sind ein Instrument zum Filtern von Geräten nach festgelegten Bedingungen. Sie können Geräteauswahlen verwenden, um mehrere Geräte zu verwalten: beispielsweise, um einen Bericht über nur diese Geräte anzuzeigen, oder um alle diese Geräte in eine andere Gruppe zu verschieben.

Kaspersky Security Center bietet eine große Zahl an *vordefinierten Auswahlen* an (z. B. **Geräte mit dem Status "Kritisch"**, **Der Schutz ist deaktiviert**, **Aktive Bedrohungen werden erkannt**). Vordefinierte Auswahlen können nicht gelöscht werden. Sie können auch zusätzliche *benutzerdefinierte Auswahlen* erstellen und konfigurieren.

In benutzerdefinierten Auswahlen können Sie den Suchbereich festlegen und alle Geräte, verwaltete Geräte oder nicht zugeordnete Geräte auswählen. Sucheinstellungen werden in den Bedingungen festgelegt. In der Geräteauswahl können Sie mehrere Bedingungen mit unterschiedlichen Sucheinstellungen erstellen. Beispielsweise können Sie zwei Bedingungen erstellen und in jeder davon unterschiedliche IP-Bereiche festlegen. Wenn mehrere Bedingungen festgelegt werden, zeigt eine Auswahl die Geräte an, die eine der Bedingungen erfüllen. Im Gegensatz dazu werden Sucheinstellungen innerhalb einer Bedingung übereinandergelegt. Wenn sowohl ein IP-Bereich als auch der Name einer installierten Anwendung in einer Bedingung festgelegt sind, werden nur jene Geräte angezeigt, bei denen sowohl die Anwendung installiert ist als auch die IP-Adresse zum festgelegten Bereich gehört.

Geräteliste einer Geräteauswahl anzeigen

In Kaspersky Security Center können Sie die Liste der Geräte für eine Geräteauswahl anzeigen.

So zeigen Sie die Geräteliste für die Geräteauswahl an:

1. Gehen Sie im Hauptmenü zum Abschnitt **Assets (Geräte)** → **Geräteauswahlen** oder **Gerätesuche und Bereitstellung** → **Geräteauswahlen**.

2. Klicken Sie in der Auswahlliste auf den Namen der entsprechenden Geräteauswahl.

   Auf der Seite wird eine Tabelle mit Informationen über die Geräte angezeigt, die in der Geräteauswahl enthalten sind.

3. Sie können die Tabelle mit den Geräten wie folgt gruppieren und filtern:

   - Klicken Sie auf das Einstellungssymbol (⚙) und wählen Sie anschließend die Spalten aus, die in der Tabelle angezeigt werden sollen.

   - Klicken Sie auf das Filter-Symbol (▽), geben Sie im aufgerufenen Menü das Filterkriterium an und wenden Sie es an.

     Die gefilterte Tabelle der Geräte wird angezeigt.

Sie können in der Geräteauswahl mehrere Geräte auswählen und auf die Schaltfläche **Neue Aufgabe** klicken, um eine Aufgabe zu erstellen, die auf diese Geräte angewendet wird.

Um die ausgewählten Geräte der Geräteauswahl in eine andere Administrationsgruppe zu verschieben, klicken Sie auf die Schaltfläche **In Gruppe verschieben** und wählen Sie anschließend die Ziel-Administrationsgruppe aus.

Geräteauswahl erstellen

Um eine Geräteauswahl zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Geräteauswahlen**.

   Eine Seite mit einer Liste von Geräteauswahlen wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Einstellungen der Geräteauswahl** wird geöffnet.

3. Geben Sie den Namen der neuen Auswahl ein.

4. Geben Sie die Gruppe mit den Geräten a, die in die Geräteauswahl aufgenommen werden sollen:

   - **Alle Geräte suchen** – Es wird nach Geräten gesucht, welche die Auswahlkriterien erfüllen und die entweder zur Gruppe **Verwaltete Geräte** oder zur Gruppe **Nicht zugeordnete Geräte** gehören.
   - **Verwaltete Geräte suchen** – Es wird nach Geräten gesucht, welche die Auswahlkriterien erfüllen und die zur Gruppe **Verwaltete Geräte** gehören.
   - **Nicht zugeordnete Geräte suchen** – Es wird nach Geräten gesucht, welche die Auswahlkriterien erfüllen und die zur Gruppe **Nicht zugeordnete Geräte** gehören.

   Sie können das Kontrollkästchen **Daten von sekundären Administrationsservern miteinbeziehen** aktivieren, um die Suche nach Geräten zu aktivieren, welche die Auswahlkriterien erfüllen und von sekundären Administrationsservern verwaltet werden.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**.
6. Wechseln Sie in das neue Fenster, geben Sie Bedingungen an, die erfüllt sein müssen, um Geräte in diese Auswahl aufzunehmen, und klicken Sie auf **OK**.
7. Klicken Sie auf die Schaltfläche **Speichern**.

Die Geräteauswahl wurde erstellt und der Liste mit Geräteauswahlen hinzugefügt.

Einstellungen einer Geräteauswahl anpassen

Um die Einstellungen für eine Geräteauswahl anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Geräteauswahlen**.

   Eine Seite mit einer Liste von Geräteauswahlen wird angezeigt.

2. Wählen Sie die relevante benutzerdefinierte Geräteauswahl aus und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Einstellungen der Geräteauswahl** wird geöffnet.

3. Klicken Sie auf der Registerkarte **Allgemein** auf den Link **Neue Bedingung**.
4. Geben Sie Bedingungen an, die erfüllt sein müssen, damit Geräte in die Auswahl aufgenommen werden.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Einstellungen werden übernommen und gespeichert.

Nachfolgende werden die Einstellungen für Bedingungen der Aufnahme von Geräten in die Auswahl beschrieben. Die Bedingungen beruhen auf dem logischen ODER: In die Auswahl werden nur Geräte aufgenommen, die mindestens eine Bedingung erfüllen.

Allgemein

Im Abschnitt **Allgemein** kann der Name der Auswahlbedingung geändert sowie bestimmt werden, ob diese Auswahlbedingung umgekehrt werden soll:

Auswahlbedingung umkehren

Diese Option ist standardmäßig deaktiviert.

Wenn Sie diese Option aktivieren, wird die vorgegebene Auswahlbedingung umgekehrt. Alle Geräte, die diese Bedingung nicht erfüllen, werden in die Auswahl aufgenommen.

Das folgende Beispiel erläutert die Logik einer Inversion:

- **Bedingung**: Auf Ihrem Gerät befindet sich ein Betriebssystem, das zu den Linux-Systemen gehört und die Build-Nummer 00.0.000 besitzt.
- **Invertierter Zustand**: Auf Ihrem Gerät befindet sich ein Betriebssystem, dass NICHT (zu den Linux-Systemen gehört und die Build-Nummer 00.0.000 besitzt), was Folgendem entspricht:

  Es ist ein Betriebssystem vorhanden, das NICHT zu den Linux-Systemen gehört ODER das NICHT die Build-Nummer 00.0.000 besitzt.

Die Auswahl umfasst also beispielhaft Geräte mit Windows-Betriebssystemen mit der Build-Nummer 00.0.000 oder Geräte mit Linux-Betriebssystemen mit einer Build-Nummer, die von 00.0.000 abweicht.

Netzwerkinfrastruktur

Im Unterabschnitt **Netzwerk** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkdaten konfigurieren:

- **Gerätename**

  Windows-Netzwerkname (NetBIOS-Name) des Geräts oder die IPv4- oder IPv6-Adresse.

- **Domäne**

  Es werden Geräte angezeigt, die zur angegebenen Windows-Domäne gehören.

- **Administrationsgruppe**

  Es werden Geräte angezeigt, die zur angegebenen Administrationsgruppe gehören.

- **Beschreibung**

  Text, der im Eigenschaftenfenster des Geräts enthalten ist: im Feld **Beschreibung** des Abschnitts **Allgemein**.

  Für die Beschreibung eines Textes im Feld **Beschreibung** sind die folgenden Zeichen zulässig:

  - Innerhalb eines Wortes:

    - *****. Dieses Zeichen ersetzt beliebige Ausdrücke mit einer beliebigen Zahl von Zeichen.

    Beispiel:

    Für die Beschreibung der Wörter **Server** und **Server-**können Sie die Zeichenfolge **Server*** verwenden.

    - **?.** Dieses Zeichen ersetzt ein beliebiges Symbol.

    Beispiel:

    Für die Beschreibung der Wörter **Regel** oder **Regeln** können Sie die Zeichenfolge **Regel?** verwenden.

    Das Zeichen ***** oder **?** kann nicht als das erste Zeichen in einer Textbeschreibung verwendet werden.

- Zur Verknüpfung mehrerer Wörter:

  - Leerzeichen: Es werden alle Geräte angezeigt, deren Beschreibung ein beliebiges der angegebenen Wörter enthält.

  Beispiel:

  Zur Beschreibung einer Phrase, die entweder das Wort **Sekundär** oder **Virtuell** enthält, können Sie die Zeichenfolge **Sekundär Virtuell** verwenden.

  - **+**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss.

  Beispiel:

  Zur Beschreibung einer Phrase, welche die beiden Wörter **Sekundär** und **Virtuell** enthält, können Sie den Ausdruck **+Sekundär+Virtuell** verwenden.

  - **-**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf.

  Beispiel:

  Zur Beschreibung einer Phrase, die das Wort **Sekundär** enthält, jedoch das Wort **Virtuell** nicht enthalten darf, können Sie den Ausdruck **+Sekundär-Virtuell** verwenden.

  - **"<Textabschnitt>"**: Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein.

  Beispiel:

  Zur Beschreibung einer Phrase, welche die Wortverbindung **Sekundärer Server** enthält, können Sie den Ausdruck **"Sekundärer Server"** verwenden.

- **IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

  Diese Option ist standardmäßig deaktiviert.

- **Verwaltung erfolgt durch anderen Administrationsserver**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte, die von anderen Administrationsservern verwaltet werden. Diese Server unterscheiden sich von dem Server, auf dem Sie die Verschiebungsregel für Geräte konfigurieren.

  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, die vom aktuellen Administrationsserver verwaltet werden.

  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

Im Unterabschnitt **Domänencontroller** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand ihrer Domänenmitgliedschaft anpassen:

- **Gerät befindet sich in einer Organisationseinheit der Domäne**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Domänenorganisationseinheit aufgenommen, die im Eingabefeld angegeben wurde.

Diese Option ist standardmäßig deaktiviert.

- **Das Gerät ist Mitglied der Domänensicherheitsgruppe**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Domänensicherheitsgruppe aufgenommen, die im Eingabefeld angegeben wurde.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Netzwerkaktivität** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkaktivitäten konfigurieren:

- **Fungiert als Verteilungspunkt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die als Verteilungspunkte fungieren, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die als Verteilungspunkte fungieren, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Verbindung mit Administrationsserver nicht trennen**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Aktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** aktiviert ist.
  - **Deaktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** deaktiviert ist.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Das Verbindungsprofil wurde gewechselt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Letzte Verbindung mit dem Administrationsserver**

  Mithilfe dieses Kontrollkästchens können Sie ein Kriterium für die Suche von Geräten anhand des Zeitpunkts der letzten Verbindung mit dem Administrationsserver ausführen.

  Wenn dieses Kontrollkästchen aktiviert ist, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, während dessen die letzte Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver hergestellt wurde. Bei Auswahl dieser Option werden in die Auswahl Geräte aufgenommen, die dem festgelegten Zeitraum entsprechen.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Neue Geräte bei der Netzwerkabfrage erkannt**

  Suche nach neuen Geräten, die während der letzten Tage bei der Netzwerkabfrage gefunden wurden.

  Wenn diese Option aktiviert ist, umfasst die Auswahl nur neue Geräte, die bei einer Gerätesuche während der im Feld **Erkennungszeitraum (Tage)** angegebenen Anzahl von Tagen gefunden wurden.

  Ist die Option deaktiviert, umfasst die Auswahl alle Geräte, die bei einer Gerätesuche gefunden wurden.

  Diese Option ist standardmäßig deaktiviert.

- **Gerät ist sichtbar**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Es werden Geräte in die Auswahl aufgenommen, die momentan im Netzwerk sichtbar sind.
  - **Nein**. Die Anwendung nimmt Geräte in die Auswahl auf, die momentan nicht im Netzwerk sichtbar sind.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Im Unterabschnitt **Cloud-Segmente** können Sie die Kriterien für die Aufnahme von Geräten in eine Auswahl anhand ihrer jeweiligen Cloud-Segmente anpassen:

- **Gerät befindet sich in einem Cloud-Segment**

  Wenn diese Option aktiviert ist, können Sie Geräte aus den Cloud-Segmenten AWS, Azure und Google auswählen.

  Wenn die Option **Untergeordnete Objekte einschließen** ebenfalls aktiviert ist, wird die Suche auf alle untergeordneten Objekte des angegebenen Segments erweitert.

  In die Suchergebnisse werden nur Geräte aus dem ausgewählten Segment aufgenommen.

- **Gerät mittels API erkannt**

  In der Dropdown-Liste können Sie wählen, ob das Gerät über API gefunden werden soll:

  - **Ja**. Das Gerät wird mithilfe der APIs von AWS, Azure oder Google erkannt.
  - **Nein**. Das Gerät kann nicht mit den APIs von AWS, Azure oder Google erkannt werden. Das bedeutet, dass sich das Gerät entweder außerhalb der Cloud-Umgebung befindet, oder dass sich das Gerät in der Cloud-Umgebung befindet, aber nicht mithilfe einer API erkannt werden kann.
  - Kein Wert. Diese Bedingung trifft nicht zu.

Gerätestatus

Im Unterabschnitt **Status des verwalteten Geräts** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Beschreibung des Gerätestatus der verwalteten Anwendung anpassen:

- **Gerätestatus**

  In dieser Dropdown-Liste können Sie einen Gerätestatus auswählen: *OK*, *Kritisch* oder *Warnung*.

- **Status des Echtzeitschutzes**

  In dieser Dropdown-Liste können Sie den Wert für den Status des Echtzeitschutzes auswählen. Geräte mit dem angegebenen Echtzeitschutz-Status werden in die Auswahl aufgenommen.

- **Beschreibung des Gerätestatus**

  In diesem Feld können Sie die Kontrollkästchen für jene Bedingungen aktivieren, auf deren Basis einem Gerät eine der folgenden Statusvarianten zugewiesen werden soll: *OK, Kritisch* oder *Warnung*.

Im Unterabschnitt **Status der Komponenten der verwalteten Programme** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Statuswerte der Komponenten der verwalteten Anwendungen anpassen:

- **Status des Schutzes vor Datenverlust**

  Suche nach Geräten anhand des Status des "Schutzes vor Datenverlust" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Schutzstatus der Server für die Zusammenarbeit**

  Suche nach Geräten anhand des Status der Komponente "Schutz der Serverzusammenarbeit" (*Unbekannt*, *Beendet*, *Wird gestartet, Angehalten*, *Wird ausgeführt*, *Fehlgeschlagen*).

- **Antiviren-Schutzstatus der Mail-Server**

  Suche nach Geräten anhand des Status des Mail-Server-Schutzes (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Status der Komponente "Endpoint Sensor"**

  Suche nach Geräten anhand des Status der Komponente "Endpoint Sensor" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

Im Unterabschnitt **Statusbeeinflussende Probleme in verwalteten Programmen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Liste von möglichen von einer verwalteten Anwendung gefundenen Problemen anpassen. Wenn zumindest ein ausgewähltes Problem auf einem Gerät existiert, wird das Gerät in die Auswahl aufgenommen. Wenn Sie ein Problem auswählen, das für mehrere Anwendungen aufgelistet ist, haben Sie die Möglichkeit, dieses Problem in allen Listen automatisch auszuwählen.

Sie können die Kontrollkästchen für die Beschreibung der Status der verwalteten Anwendungen aktivieren, bei deren Empfang die Geräte in die Auswahl aufgenommen werden. Wenn Sie einen Status auswählen, der für mehrere Anwendungen aufgelistet ist, haben Sie die Möglichkeit, diesen Status in allen Listen automatisch auszuwählen.

Details zum System

Im Abschnitt **Betriebssystem** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl auf der Grundlage des darauf installierten Betriebssystems anpassen.

- **Plattformtyp**

  Ist das Kontrollkästchen aktiviert, können Sie Betriebssysteme in der Liste auswählen. Geräte, auf denen die angegebenen Betriebssysteme installiert sind, werden in die Suchergebnisse aufgenommen.

- **Service Pack-Version des Betriebssystems**

  In diesem Feld können Sie die Service Pack-Version (im Format *X.Y*) des Betriebssystems angeben, die bestimmt, wie die Verschiebungsregel auf das Gerät angewendet wird. Standardmäßig ist keine Version angegeben.

- **Bitzahl des Betriebssystems**

  In dieser Dropdown-Liste können Sie die Architektur des Betriebssystems auswählen, die vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird (**Unbekannt**, **x86**, **AMD64**, **IA64**). Standardmäßig ist in dieser Liste keine Variante ausgewählt, die Architektur des Betriebssystems ist nicht angegeben.

- **Build-Version des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Versionsnummer des Betriebssystems. Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Suche nach allen Versionsnummern mit Ausnahme der angegebenen anpassen.

- **Releasenummer des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Release-Identifikator (ID) des Betriebssystems Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-ID haben muss. Sie können auch eine Suche nach allen Release-ID-Nummern mit Ausnahme der angegebenen anpassen.

Auf der Registerkarte **Virtuelle Maschinen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anpassen, je nachdem, ob diese Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- **Ist eine virtuelle Maschine**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Nicht definiert**.
  - **Nein**. Die gesuchten Geräte dürfen keine virtuellen Maschinen sein.
  - **Ja**. Die gesuchten Geräte müssen virtuelle Maschinen sein.

- **Typ der virtuellen Maschine**

  In der Dropdown-Liste können Sie den Hersteller der virtuellen Maschine auswählen.

  Die Dropdown-Liste ist verfügbar, wenn die Werte **Ja** oder **Unwichtig** in der Dropdown-Liste **Dies ist eine virtuelle Maschine** gewählt wurden.

- **Teil einer Virtual Desktop Infrastructure (VDI)**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Nicht definiert**.
  - **Nein**. Die gesuchten Geräte dürfen kein Teil der Virtual Desktop Infrastructure (VDI) sein.
  - **Ja**. Die gesuchten Geräte müssen Teil der Virtual Desktop Infrastructure (VDI) sein.

Im Unterabschnitt **Hardware-Register** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der auf ihnen installierten Hardware anpassen:

Stellen Sie sicher, dass das Tool "lshw" auf den Linux-Geräten installiert ist, von denen Sie die Hardwaredetails abrufen möchten. Die von virtuellen Maschinen abgerufenen Hardwaredetails können je nach verwendetem Hypervisor unvollständig sein.

- **Gerät**

  In dieser Dropdown-Liste können Sie einen Einheitentyp auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Namen eines Herstellers der Einheit auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- **Gerätename**

  Name des Geräts im Windows-Netzwerk. Ein Gerät mit dem angegebenen Namen wird in die Auswahl aufgenommen.

- **Beschreibung**

  Beschreibung des Geräts oder der Hardware. Geräte mit der in diesem Feld angegebenen Beschreibung werden in die Auswahl aufgenommen.

  Eine Beschreibung in beliebiger Form kann im Fenster Geräteeigenschaften eingegeben werden. Im Feld wird die Volltextsuche unterstützt.

- **Gerätehersteller**

  Bezeichnung des Geräteherstellers. Geräte, die vom angegebenen Hersteller produziert wurden, werden in die Auswahl aufgenommen.

  Der Name des Herstellers kann im Fenster Geräteeigenschaften eingegeben werden.

- **Seriennummer**

  Hardware mit in diesem Feld angegebener Seriennummer wird in die Auswahl aufgenommen.

- **Inventarnummer**

  Hardware mit in diesem Feld angegebener Inventarnummer wird in die Auswahl aufgenommen.

- **Benutzer**

  Hardware des in diesem Feld angegebenen Benutzers wird in die Auswahl aufgenommen.

- **Ort**

  Standort des Geräts bzw. der Hardware (z. B. im Büro oder in der Filiale). Computer oder andere Geräte am in diesem Feld angegebenen Ort werden in die Auswahl aufgenommen.

  Der Ort der Hardware kann in beliebiger Form im Hardware-Eigenschaftenfenster eingegeben werden.

- **CPU-Taktrate in MHz, von**

  Die minimale Taktrate einer CPU. Geräte mit einer CPU, deren Taktrate dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **CPU-Taktrate MHz, bis**

  Die maximale Taktrate einer CPU. Geräte mit einer CPU, deren Taktrate dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Anzahl virtueller CPU-Kerne, von**

  Die minimale Anzahl an virtuellen CPU-Kernen. Geräte mit einer CPU, deren Anzahl an Kernen dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Anzahl virtueller CPU-Kerne, bis**

  Die maximale Anzahl an virtuellen CPU-Kernen. Geräte mit einer CPU, deren Anzahl an Kernen dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB), von**

  Die minimale Größe der Festplatte des Geräts. Geräte mit Festplatten, deren Größe dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB), bis**

  Die maximale Größe der Festplatte des Geräts. Geräte mit Festplatten, deren Größe dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **RAM-Größe in MB, von**

  Die minimale Größe des Arbeitsspeichers des Geräts. Geräte mit Arbeitsspeicher, der dem Größenbereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Speichergröße MB, bis**

  Die minimale Größe des Arbeitsspeichers des Geräts. Geräte mit Arbeitsspeicher, der dem Größenbereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

Details zu Drittherstellersoftware

Im Unterabschnitt **Programm-Registry** können Sie die Kriterien für die Aufnahme von Geräten anhand von installierten Anwendungen anpassen:

- **Programmname**

  In dieser Dropdown-Liste können Sie einen Anwendungsnamen auswählen. Die Geräte, auf denen diese Anwendung installiert ist, werden in die Auswahl aufgenommen.

- **Programmversion**

  Geben Sie in diesem Eingabefeld die Version der ausgewählten Anwendung ein.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Hersteller der auf dem Gerät installierten Anwendung auswählen.

- **Programmstatus**

  Dropdown-Liste, in der Sie den Status der Anwendung auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen die angegebene Anwendung abhängig vom ausgewählten Status installiert bzw. nicht installiert ist, werden in die Auswahl aufgenommen.

- **Nach Update suchen**

  Wenn diese Option aktiviert ist, erfolgt die Suche anhand der Updatedaten der auf den Geräten installierten Anwendungen. Nachdem Sie das Kontrollkästchen aktiviert haben, ändern sich die Felder **Programmname**, **Programmversion** und **Programm-Status** in **Update-Name**, **Update-Version** und **Status**.

  Diese Option ist standardmäßig deaktiviert.

- **Name der inkompatiblen Sicherheitsanwendung**

  In dieser Dropdown-Liste können Sie Sicherheitsanwendungen von Drittanbietern auswählen. Bei der Suche werden Geräte in die Auswahl aufgenommen, auf denen die ausgewählte Anwendung installiert wurde.

- **Programm-Tag**

  In dieser Dropdown-Liste können Sie ein Anwendungs-Tag auswählen. Alle Geräte, auf denen Anwendungen installiert sind, die das ausgewählte Tag in der Beschreibung haben, werden in die Geräteauswahl aufgenommen.

- **Auf Geräte ohne angegebene Tags anwenden**

  Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in die Auswahl aufgenommen.

  Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Schwachstellen und Updates** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Quelle der Windows-Updates anpassen:

WUA wurde auf den Administrationsserver umgeschaltet

In dieser Dropdown-Liste können Sie eine der folgenden Varianten der Suche auswählen:

- **Ja**. Bei Auswahl dieser Option werden Geräte in die Suchergebnisse aufgenommen, die Windows-Updates vom Administrationsserver herunterladen.
- **Nein**. Bei Auswahl dieser Option werden Geräte in die Ergebnisse aufgenommen, die Windows-Updates von einer anderen Quelle herunterladen.

Details zu Programmen von Kaspersky

Im Unterabschnitt **Programme von Kaspersky** können Sie die Kriterien für die Aufnahme von Geräten anhand der ausgewählten verwalteten Anwendung konfigurieren:

- **Programmname**

  In der Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl wählen, wenn die Suche anhand des Namens der Kaspersky-Anwendung erfolgt.

  In der Liste sind nur die Anwendungen aufgeführt, für die Verwaltungs-Plug-ins im Administrator-Arbeitsplatz installiert sind.

  Wurde keine Anwendung gewählt, wird kein Kriterium angewandt.

- **Programmversion**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach Versionsnummer der Kaspersky-Anwendung erfolgt.

  Wurde keine Versionsnummer angegeben, wird kein Kriterium angewandt.

- **Name des kritischen Updates**

  Dropdown-Liste, in der Sie den Status des Programms auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen das angegebene Programm abhängig vom ausgewählten Status installiert bzw. nicht installiert ist, werden in die Auswahl aufgenommen.

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach Programmnamen oder der Update-Paketnummer erfolgt.

  Ist dieses Feld leer, wird kein Kriterium angewandt.

- **Wählen Sie den Zeitraum für das letzte Modul-Update**

  Mithilfe dieser Option können Sie ein Kriterium für die Suche nach Geräten nach Uhrzeit des letzten Updates der Anwendungsmodule angeben, die auf den Geräten installiert wurden.

  Ist das Kontrollkästchen aktiviert, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, in dem das letzte Update der auf den Geräten installierten Anwendungsmodule ausgeführt wurde.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Das Gerät wird durch den Administrationsserver verwaltet**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, die über Kaspersky Security Center verwaltet werden:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn sie über Kaspersky Security Center verwaltet werden.
  - **Nein**. Das Programm nimmt Geräte in die Auswahl auf, wenn sie nicht über Kaspersky Security Center verwaltet werden.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Sicherheitsanwendung wurde installiert**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, auf denen eine Sicherheitsanwendung installiert wurde:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn auf ihnen eine Sicherheitsanwendung installiert ist.
  - **Nein**. Die Anwendung nimmt alle Geräte in die Auswahl auf, die keine Sicherheitsanwendung installiert haben.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Im Unterabschnitt **Antiviren-Schutz** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand des Schutzstatus anpassen:

- **Veröffentlichung der Datenbanken**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Veröffentlichungsdatum der Antiviren-Datenbanken. In den Eingabefeldern können Sie den Zeitraum festlegen, anhand dessen die Suche ausgeführt werden soll.

  Diese Option ist standardmäßig deaktiviert.

- **Anzahl der Datenbank-Einträge**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach der Anzahl der Datenbank-Einträge. In den Eingabefeldern können Sie den unteren und oberen Wert für die Anzahl der Einträge in der Antiviren-Datenbank festlegen.

  Diese Option ist standardmäßig deaktiviert.

- **Letzte Virensuche**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Zeitpunkt der letzten Schadsoftware-Untersuchung. In den Eingabefeldern können Sie den Zeitraum festlegen, in dem die Schadsoftware-Untersuchung zum letzten Mal erfolgte.

  Diese Option ist standardmäßig deaktiviert.

- **Gefundene Bedrohungen**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach der Anzahl der gefundenen Viren. In den Eingabefeldern können Sie den unteren und oberen Wert für die Anzahl der gefundenen Viren festlegen.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Verschlüsselung** können Sie das Kriterium für die Aufnahme von Geräten anhand des ausgewählten Verschlüsselungsalgorithmus konfigurieren:

Verschlüsselungsalgorithmus

Standard des symmetrischen Algorithmus der Blockverschlüsselung Advanced Encryption Standard (AES). In der Dropdown-Liste können Sie die Länge des Chiffrierschlüssels (56 Bit, 128 Bit, 192 Bit oder 256 Bit) auswählen.

AES56, *AES128*, *AES192*, *AES256*.

Der Unterabschnitt **Programmkomponenten** enthält eine Liste mit Komponenten von Anwendungen, für die entsprechende Verwaltungs-Plug-ins in Kaspersky Security Center Web Console installiert sind.

Im Unterabschnitt **Programmkomponenten** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status und Versionsnummern der Komponenten festlegen, die sich auf die ausgewählte Anwendung beziehen:

- **Status**

  Suche nach Geräten anhand des Status der Komponente, der von einer Anwendung an den Administrationsserver gesendet wurde. Sie können einen der folgenden Statuswerte auswählen: *Keine Daten, Beendet*, *Angehalten*, *Wird gestartet*, *Wird ausgeführt, Fehlgeschlagen*, *Nicht installiert, Von der Lizenz nicht unterstützt*. Wenn die ausgewählte Komponente der auf einem verwalteten Gerät installierten Anwendung den angegebenen Status aufweist, wird das Gerät bei der Geräteauswahl berücksichtigt.

Von Anwendungen gesendete Status:

- *Beendet* – Die Komponente ist deaktiviert und funktioniert momentan nicht.
- *Angehalten* – Die Komponente wird angehalten, z. B. nachdem der Benutzer den Schutz in der verwalteten Anwendung angehalten hat.
- *Wird gestartet* – Die Komponente wird gerade initialisiert.
- *Wird ausgeführt* – Die Komponente ist aktiviert und funktioniert ordnungsgemäß.
- *Fehlgeschlagen* – Während des Betriebs der Komponente ist ein Fehler aufgetreten.
- *Nicht installiert*–Der Benutzer hat die Komponente während der Konfiguration der benutzerdefinierten Installation der Anwendung nicht für die Installation ausgewählt.
- *Von der Lizenz nicht unterstützt* – Die Lizenz gilt nicht für die ausgewählte Komponente.

Im Gegensatz zu anderen Statuswerten wird der Statuswert *Keine Daten* nicht von Anwendungen versendet. Diese Option zeigt, dass die Anwendungen über keine Informationen über den ausgewählten Status der Komponente aufweisen. Dies kann beispielsweise der Fall sein, wenn die ausgewählte Komponente zu keiner der auf dem Gerät installierten Anwendungen gehört oder wenn das Gerät ausgeschaltet ist.

- **Version**

  Suche nach Geräten anhand der Versionsnummer der in der Liste ausgewählten Komponente. Sie können eine Versionsnummer eingeben, beispielsweise `3.4.1.0`, und dann festlegen, ob die ausgewählte Komponente eine gleich, frühere oder spätere Version aufweisen muss. Sie können auch eine Suche nach allen Versionen mit Ausnahme der angegebenen anpassen.

Tags

Im Abschnitt **Tags** können Sie Bedingungen für die Aufnahme von Geräten in die Auswahl nach Schlüsselworten (Tags) anpassen, die zuvor zu den Beschreibungen der verwalteten Geräte hinzugefügt wurden:

Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft

Ist die Option aktiviert, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibungen zumindest einer der gewählten Tags vorhanden ist.

Ist die Option deaktiviert, werden in den Suchergebnissen nur Geräte angezeigt, in deren Beschreibungen alle gewählten Tags vorhanden sind.

Diese Option ist standardmäßig deaktiviert.

Um dem Kriterium Tags hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie die Tags aus, indem Sie auf das Eingabefeld **Tag** klicken. Geben Sie an, ob die Geräte mit den ausgewählten Tags in die Geräteauswahl aufgenommen oder davon ausgeschlossen werden sollen.

- **Alle Geräte mit diesem Tag**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

  Diese Variante ist standardmäßig ausgewählt.

- **Alle Geräte ohne dieses Tag**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag nicht vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

Benutzer

Auf der Registerkarte **Benutzer** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Benutzerkonten anpassen, die sich am Betriebssystem angemeldet haben.

- **Letzter am System angemeldeter Benutzer**

  Wenn diese Option aktiviert ist, können Sie das Benutzerkonto für die Konfiguration des Kriteriums auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der ausgewählte Benutzer zuletzt angemeldet hat.

- **Benutzer, der sich mindestens einmal am System angemeldet hat**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer mindestens einmal im System angemeldet hat.

Geräteliste einer Geräteauswahl exportieren

Mit der Kaspersky Security Center können Sie Informationen über Geräte aus einer Geräteauswahl speichern und in eine csv- oder txt-Datei exportieren.

So exportieren Sie die Geräteliste der Geräteauswahl:

1. Öffnen Sie die Tabelle mit den Geräten aus der Geräteauswahl.
2. Verwenden Sie eine der folgenden Methoden, um die Geräte auszuwählen, die Sie exportieren möchten:
   - Um nur bestimmte Geräte auszuwählen, aktivieren Sie die entsprechenden Kontrollkästchen neben diesen.
   - Um alle Geräte auf der aktuellen Tabellenseite auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Gerätetabelle und aktivieren Sie anschließend das Kontrollkästchen **Alle auf aktueller Seite** auswählen.
   - Um alle Geräte aus der gesamten Tabelle auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Gerätetabelle und aktivieren Sie dann das Kontrollkästchen **Alle auswählen**.
3. Klicken Sie auf die Schaltfläche **In csv-Datei exportieren** oder **In txt-Datei exportieren**. Alle Informationen zu den in der Tabelle enthaltenen ausgewählten Geräten werden exportiert.

Beachten Sie, dass bei einem auf die Tabelle angewendeten Filterkriterium nur die gefilterten Daten aus den angezeigten Spalten exportiert werden.

Geräte in der Auswahl aus Administrationsgruppen löschen

Bei der Arbeit mit einer Geräteauswahl können Sie Geräte direkt in der Auswahl aus den Administrationsgruppen löschen, ohne auf die Administrationsgruppen zu wechseln, aus denen die Geräte gelöscht werden sollen.

Um Geräte aus Administrationsgruppen zu löschen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Geräteauswahlen** oder zu **Gerätesuche und Bereitstellung** → **Geräteauswahlen**.
2. Klicken Sie in der Auswahlliste auf den Namen der entsprechenden Geräteauswahl.

   Auf der Seite wird eine Tabelle mit Informationen über die Geräte angezeigt, die in der Geräteauswahl enthalten sind.
3. Wählen Sie die Geräte aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.

   Daraufhin werden die gewählten Geräte aus den Administrationsgruppen gelöscht, zu denen sie gehörten.

Geräte-Tags

Kaspersky Security Center erlaubt, den Geräten *Tags* zuzuweisen. Ein Tag ist die Bezeichnung eines Geräts und es kann für die Gruppierung, Beschreibung oder Suche von Geräten verwendet werden. Die den Geräten zugewiesenen Tags können beim Erstellen von Geräteauswahlen, bei der Suche nach Geräten und bei der Gerätezuordnung anhand von Administrationsgruppen verwendet werden.

Die Tags können den Geräten manuell oder automatisch zugewiesen werden. Wenn Sie ein einzelnes Gerät mit Tags versehen möchten, können Sie die manuelle Tag-Zuweisung verwenden. Die automatische Tag-Zuweisung wird von Kaspersky Security Center auf eine der folgenden Arten durchgeführt:

- In Übereinstimmung mit den angegebenen Regeln zur Tag-Zuweisung.
- Durch eine Anwendung.

> Es wird nicht empfohlen, verschiedene Arten der Tag-Zuweisung zu verwenden, um dasselbe Tag zuzuweisen. Wenn das Tag beispielsweise durch die Regel zugewiesen wird, wird es nicht empfohlen, dieses Tag den Geräten manuell zuzuweisen.

Wenn die Tags durch Regeln zugewiesen werden, bekommen die Geräte die Tags zugewiesen, wenn die festgelegten Regeln erfüllt sind. Jedem Tag entspricht eine separate Regel. Die Regeln können auf die Netzwerkeigenschaften des Geräts, das Betriebssystem, die auf dem Gerät installierten Programmen und andere Eigenschaften des Geräts angewendet werden. Wenn Sie beispielsweise eine Hybridinfrastruktur aus physischen Maschinen, Amazon EC2-Instanzen und virtuellen Microsoft Azure-Maschinen haben, können Sie eine Regel einrichten, die allen virtuellen Microsoft Azure-Maschinen das Tag `[Azure]` zuweist. Diese Tag kann anschließend beim Erstellen von Geräteauswahlen verwendet werden, um alle virtuellen Microsoft Azure-Maschinen zu sortieren und ihnen eine Aufgabe zuzuweisen.

> Sie können pro Tag nur eine Regel für die automatische Tag-Zuweisung hinzufügen. Wenn Sie eine neue Regel für dasselbe Tag erstellen, wird die vorherige ersetzt.

Ein Tag wird in den folgenden Fällen automatisch vom Gerät entfernt:

- Wenn das Gerät nicht mehr die Bedingungen der Regel erfüllt, die das Tag zuweist.
- Wenn die Regel, die das Tag zuweist, deaktiviert oder gelöscht wird.

Die Liste der Tags und die Liste mit Regeln sind auf jedem Administrationsserver unabhängig von allen anderen Administrationsservern, einschließlich des primären Administrationsservers und der untergeordneten virtuellen Administrationsserver. Eine Regel wird nur auf Geräte des gleichen Administrationsservers angewendet, auf dem die Regel erstellt wurde.

Geräte-Tag erstellen

Um ein Geräte-Tag zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Tags** → **Tags des Geräts**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   Ein neues Tag-Fenster öffnet sich.
3. Geben Sie im Feld **Tag** den Namen des Tags ein.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das neue Tag wird in der Liste der Geräte-Tags angezeigt.

Geräte-Tag umbenennen

Um ein Geräte-Tag umzubenennen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Tags** → **Tags des Geräts**.
2. Klicken Sie auf den Namen des Tags, das Sie umbenennen möchten.
   Ein Fenster mit den Tag-Eigenschaften wird geöffnet.
3. Ändern Sie im Feld **Tag** den Tag-Namen.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das aktualisierte Tag wird in der Liste der Geräte-Tags angezeigt.

Geräte-Tag löschen

Um ein Geräte-Tag zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Tags** → **Tags des Geräts**.
2. Wählen Sie in der Liste das Geräte-Tag aus, das Sie löschen möchten.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **Ja**.

   Das Geräte-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Geräten entfernt, denen es zugewiesen war.

> Das von Ihnen gelöschte Tag wird nicht automatisch aus den Regeln für die automatische Tag-Zuweisung entfernt. Nach dem Löschen des Tags wird es nur dann einem neuen Gerät zugewiesen, wenn das Gerät die Bedingungen der Regel erfüllt, die das Tag zuweist.

> Das gelöschte Tag wird nicht automatisch vom Gerät entfernt, wenn dieses Tag dem Gerät von einer Anwendung oder einem Administrationsagenten zugewiesen wurde. Verwenden Sie das Tool "klscflag", um solche Tags zu verwalten.

Geräte mit zugewiesenen Tags anzeigen

So zeigen Sie Geräte an, denen ein Tag zugewiesen ist:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Tags** → **Tags des Geräts**.

2. Klicken Sie auf den Link **Geräte anzeigen** neben dem Tag, für das Sie zugewiesene Geräte anzeigen möchten.

   Sie werden zum Abschnitt **Verwaltete Geräte** des Hauptmenüs weitergeleitet, wobei die Geräte nach dem Tag gefiltert sind, auf dessen **Geräte anzeigen**-Link Sie geklickt haben.

3. Wenn Sie zur Liste der Geräte-Tags zurückzukehren möchten, klicken Sie in Ihrem Browser auf die Schaltfläche **Zurück**.

Nachdem Sie die Geräte mit dem zugewiesenen Tag angezeigt haben, können Sie entweder ein neues Tag erstellen und zuweisen oder das vorhandene Tag anderen Geräten zuweisen. In diesem Fall müssen Sie den Filterung nach Tag entfernen, die Geräte auswählen und anschließend das Tag zuweisen.

Tags anzeigen, die einem Gerät zugewiesen sind

So zeigen Sie einem Gerät zugewiesene Tags an:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

2. Klicken Sie auf den Namen des Geräts, dessen Tags Sie anzeigen möchten.

3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Tags** aus.

   Die Liste der dem ausgewählten Gerät zugewiesenen Tags wird angezeigt. In der Spalte **Tag zugewiesen** können Sie anzeigen, wie das Tag zugewiesen wurde.

In der Werkzeugleiste sind folgende Aktionen möglich:

- Dem Gerät ein anderes Tag zuweisen.
- Ein bereits zugewiesenes Tag entfernen.
- Alle Geräte-Tags anzeigen, die auf dem Administrationsserver vorhanden sind.

Sie können die zugewiesenen Tags nicht lokal auf dem Gerät anzeigen.

Tags einem Gerät manuell zuweisen

So weisen Sie einem Gerät ein Tag manuell zu:

1. Zeigen Sie dem Gerät zugeordnete Tags an, dem Sie einen anderen Tag zuweisen möchten.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Führen Sie im folgenden Fenster einen der folgenden Schritte aus:
   - Um ein neues Tag zu erstellen und zuzuweisen, wählen Sie **Neues Tag erstellen** und geben Sie den Namen des neuen Tags ein.
   - Um ein vorhandenes Tag auszuwählen, wählen Sie **Vorhandenes Tag zuordnen** und dann in der Dropdown-Liste das gewünschte Tag.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

   Das ausgewählte Tag wird dem Gerät zugewiesen.

Zugewiesene Tags von einem Gerät entfernen

So entfernen Sie ein Tag von einem Gerät:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen des Geräts, dessen Tags Sie anzeigen möchten.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Tags** aus.
4. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie entfernen möchten.

5. Klicken Sie am oberen Ende der Liste auf die Schaltfläche **Tag-Zuweisung aufheben?**.

6. Klicken Sie im folgenden Fenster auf **Ja**.

Das Tag wurde vom Gerät entfernt.

Das nicht zugewiesene Geräte-Tag wird nicht gelöscht. Bei Bedarf können Sie es manuell löschen.

Sie können Tags, die dem Gerät von Anwendungen oder Administrationsagenten zugewiesen wurden, nicht manuell entfernen. Um diese Tags zu verwalten, verwenden Sie das Tool "klscflag".

Regeln für das automatische Zuweisen von Tags an Geräten anzeigen

So zeigen Sie Regeln für die automatischer Zuweisung von Tags an Geräte an:

Führen Sie eine beliebige der folgenden Aktionen aus:

- Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Tags** → **Regeln für die automatische Tag-Zuweisung**.
- Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Tags** → **Tags des Geräts** und klicken Sie anschließend auf den Link **Regeln für die automatische Tag-Zuweisung einrichten**.
- Zeigen Sie die Tags an, die einem Gerät zugeordnet sind, und klicken Sie dann auf **Einstellungen**.

Die Liste der Regeln für die automatische Tag-Zuweisung von Geräten wird angezeigt.

Regeln für das automatische Zuweisen von Tags an Geräte bearbeiten

So bearbeiten Sie die Regeln für das automatische Zuweisen von Tags an Geräte:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.

2. Klicken Sie auf den Namen der Regel, die Sie bearbeiten möchten.
   Es wird ein Fenster zum Erstellen neuer Regeln geöffnet.

3. Bearbeiten Sie die allgemeinen Eigenschaften der Regel:

   a. Ändern Sie im Feld **Regelname** den Regelnamen.
      Der Name darf nicht mehr als 256 Zeichen enthalten.

   b. Führen Sie eine beliebige der folgenden Aktionen aus:

      - Aktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel aktiviert** umschalten.
      - Deaktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel deaktiviert** umschalten.

4. Führen Sie eine beliebige der folgenden Aktionen aus:

   - Um eine neue Bedingung hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**, um im sich öffnenden Fenster die Einstellungen der neuen Bedingung festzulegen.
   - Um eine vorhandene Bedingung zu bearbeiten, klicken Sie auf den Namen dieser Bedingung und bearbeiten Sie dann die Einstellungen der Bedingung.
   - Um eine Bedingung zu löschen, aktivieren Sie das Kontrollkästchen neben dem Namen dieser Bedingung und klicken Sie dann auf **Löschen**.

5. Klicken Sie im Fenster zum Einstellen der Bedingung auf **OK**.

6. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die bearbeitete Regel wird in der Liste angezeigt.

Regeln für das automatische Zuweisen von Tags an Geräte erstellen

So erstellen Sie Regeln für das automatische Zuweisen von Tags an Geräte:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Es wird ein neues Fenster zum Erstellen von Regeln geöffnet.

3. Passen Sie die allgemeinen Eigenschaften der Regel an:

   a. Geben Sie im Feld **Regelname** den Regelnamen ein.

   Der Name darf nicht mehr als 256 Zeichen enthalten.

   b. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel aktiviert** umschalten.
   - Deaktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel deaktiviert** umschalten.

   c. Geben Sie im Feld **Tag** den neuen Namen des Geräte-Tags ein oder wählen Sie eins der vorhandenen Geräte-Tags aus der Liste aus.

   Der Name darf nicht mehr als 256 Zeichen enthalten.

4. Klicken Sie im Abschnitt "Bedingungen" auf die Schaltfläche **Hinzufügen**, um eine neue Bedingung hinzufügen.

   Ein neues Fenster zum Einstellen von Bedingungen wird geöffnet.

5. Geben Sie den Namen der Bedingung ein.

   Der Name darf nicht mehr als 256 Zeichen enthalten. Der Name darf sich innerhalb einer Regel nicht wiederholen.

6. Passen Sie das Auslösen der Regel entsprechend den folgenden Bedingungen an: Es können mehrere Bedingungen ausgewählt werden.

   - **Netzwerk** – Netzwerkeigenschaften des Gerätes (beispielsweise Gerätename im Windows-Netzwerk oder Zugehörigkeit des Gerätes zu einer Domäne oder einem IP-Subnetz).

     Wenn für die Datenbank, die Sie für Kaspersky Security Center verwenden, die Unterscheidung zwischen Groß- und Kleinschreibung festgelegt ist, behalten Sie die Groß- und Kleinbuchstaben bei, wenn Sie einen DNS-Namen für das Gerät angeben. Andernfalls funktioniert Regel der automatischen Tag-Zuweisung nicht.

   - **Programme** – Vorhandensein des Administrationsagenten auf dem Gerät, Typ, Version und Betriebssystemarchitektur.
   - **Virtuelle Maschinen** – Das Gerät gehört zu einem speziellen Typ für virtuelle Maschinen.
   - **Domänencontroller** – Vorhandensein des Gerätes in einer Active Directory-Organisationseinheit und Zugehörigkeit des Gerätes zu einer Active Directory-Gruppe.
   - **Programm-Registry** – Vorhandensein von Programmen verschiedener Hersteller auf dem Gerät.

7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

   Falls erforderlich, können mehrere Bedingungen für eine Regel festgelegt werden. In diesem Fall wird den Geräten das Tag zugewiesen, wenn mindestens eine der Bedingungen erfüllt wird.

8. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die erstellte Regel wird auf Geräten ausgeführt, die vom ausgewählten Administrationsserver verwaltet werden. Wenn die Einstellungen für das Gerät den Bedingungen der Regel entsprechen, wird diesem Gerät das Tag zugewiesen.

Später wird eine Regel in folgenden Fällen angewendet:

- Automatisch und regelmäßig, abhängig von der Serverauslastung
- Nachdem Sie die Regel bearbeitet haben
- Wenn Sie die Regel manuell ausführen
- Wenn der Administrationsserver erkennt, dass entweder die Einstellungen eines Gerätes geändert wurden, das den Regelbedingungen entspricht, oder dass die Einstellungen einer Gruppe geändert wurden, die ein solches Gerät enthält.

Sie können mehrere Regeln zur Zuweisung von Tags erstellen. Einem Gerät können mehrere Tags zugewiesen werden, falls Sie mehrere Regeln zur Zuweisung von Tags erstellt haben und Bedingungen dieser Regeln gleichzeitig erfüllt sind. Sie können die Liste aller zugewiesenen Tags in den Eigenschaften des Geräts einsehen.

Regeln für das automatische Zuweisen von Tags an Geräte ausführen

Wird eine Regel ausgeführt, wird das in den Eigenschaften dieser Regel angegebene Tag den Geräten zugewiesen, welche die in den Eigenschaften derselben Regel angegeben Bedingungen erfüllen. Sie können nur aktivierte Regeln ausführen.

So führen Sie die Regeln für das automatische Zuweisen von Tags an Geräte aus:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.
2. Aktivieren Sie die Kontrollkästchen neben den aktivierten Regeln, die Sie ausführen möchten.
3. Klicken Sie auf die Schaltfläche **Regel ausführen**.

Die ausgewählten Regeln werden ausgeführt.

Regeln für das automatische Zuweisen von Tags an Geräte löschen

So löschen Sie die Regeln für das automatische Zuweisen von Tags an Geräte:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.
2. Aktivieren Sie die Kontrollkästchen neben der Regel, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster erneut auf **Löschen**.

Die ausgewählte Regel wird gelöscht. Das Tag, das in den Eigenschaften dieser Regel angegeben wurde, wird nicht von allen Geräten entfernt, denen es zugewiesen wurde.

Das nicht zugewiesene Geräte-Tag wird nicht gelöscht. Bei Bedarf können Sie es manuell löschen.

Verwalten von Geräte-Tags mit dem Tool klscflag

Um einem Gerät einen Satz an Tags zuzuweisen, müssen Sie das Tool "klscflag" auf dem Client-Gerät ausführen, dem Sie die Tags zuweisen möchten.

Das Tool "klscflag" überschreibt die vorhandenen Tags, die dem Gerät zugewiesen sind. Dies bedeutet, dass Sie Tags hinzufügen oder entfernen können, indem Sie im Befehl den jeweiligen Satz an Tags angeben. Das Tool besitzt keine separaten Befehle zum Hinzufügen oder Entfernen einzelner Tags. Stattdessen ändern Sie den gesamten Satz an Tags.

Wenn Sie in Befehlen wie "klscflag" verschiedene Tag-Namen angeben, wird es empfohlen, einen einheitlichen Ansatz in Bezug auf die Groß- und Kleinschreibung zu wählen (z. B. ausschließlich Großbuchstaben für alle Tags). Je nach Konfiguration des DBMS hilft die ausschließliche Verwendung von Großbuchstaben bei der Vermeidung von Problemen mit Tags, die sich lediglich in der Groß- und Kleinschreibung unterscheiden.

So weisen Sie Ihrem Gerät Tags mithilfe des Tools klscflag zu:

1. Führen Sie die Windows-Eingabeaufforderung als Administrator aus und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsagent installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ NetworkAgent".

2. Geben Sie einen der folgenden Befehle ein:

   - So weisen Sie einen Satz mit Tags zu:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" TAG-NAME_1 \",\" TAG-NAME_2 \",\" TAG-NAME_3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     wobei `[\" TAG-NAME_1 \",\" TAG-NAME_2 \",\" TAG-NAME_3 \"]` für die Liste der Tags steht, die Sie Ihrem Gerät zuweisen möchten.

     Wenn Sie die eckigen Klammern leer lassen, werden alle Tags vom Gerät entfernt:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - So weisen Sie einem vorhandenen Satz mit Tags ein neues Tag zu:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NEUER-TAG-NAME \",\" TAG-NAME_1 \",\" TAG-NAME_2 \",\" TAG-NAME_3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     wobei `NEUER-TAG-NAME` für den Namen des Tags steht, das Sie Ihrem Gerät zuweisen möchten, und `TAG-NAME_1`, `TAG-NAME_2` und `TAG-NAME_3` die Namen der Tags sind, die dem Gerät bereits zugewiesen sind.

   - Um ein bestimmtes Tag zu entfernen, ohne dabei andere, dem Gerät bereits zugewiesene, Tags zu entfernen, führen Sie den Befehl mit dem aktualisierten Satz an Tags aus.

     Wenn Ihre aktuellen Tags beispielsweise `TAG-NAME_1`, `TAG-NAME_2` und `TAG-NAME_3` lauten und Sie `TAG-NAME_2` entfernen möchten, führen Sie den folgenden Befehl aus:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" TAG-NAME_1 \",\" TAG-NAME_3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Starten Sie den Dienst des Administrationsagenten neu.

   Das Tool "klscflag" weist Ihrem Gerät die angegebenen Tags zu.

4. Wenn Sie sicherstellen möchten, dass die Tags durch das Tool "klscflag" erfolgreich zugewiesen wurden, zeigen Sie die dem Gerät zugewiesenen Tags an.

Alternativ können Sie Geräte-Tags manuell zuweisen.

Richtlinien und Richtlinienprofile

In Kaspersky Security Center Web Console können Sie Richtlinien für Kaspersky-Anwendungen erstellen. In diesem Abschnitt werden Richtlinien und Richtlinienprofile beschrieben, und Sie erhalten Anweisungen für deren Erstellung und Änderung.

Über Richtlinien und Richtlinienprofile

Eine *Richtlinie* besteht aus einer Reihe von Einstellungen für Kaspersky-Anwendungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Anwendungen auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center bietet eine einzelne Richtlinie für jede Kaspersky-Anwendung in einer Administrationsgruppe. Eine Richtlinie besitzt einen der folgenden Statuswerte (siehe Abbildung unten):

Status der Richtlinie

Status	Beschreibung
Aktiv	Die aktuelle Richtlinie, die auf das Gerät angewendet wird. In jeder Administrationsgruppe kann nur eine Richtlinie für eine Kaspersky-Anwendung aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für eine Kaspersky-Anwendung an.
Inaktiv	Eine Richtlinie, die derzeit nicht auf ein Gerät angewendet wird.
Für mobile Benutzer	Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

Richtlinien funktionieren gemäß den folgenden Regeln:

- Für eine einzelne Anwendung können mehrere Richtlinien mit unterschiedlichen Werten konfiguriert werden.
- Für das aktuelle Programm kann nur eine Richtlinie aktiv sein.
- Bei Auftreten eines bestimmten Ereignisses können Sie eine deaktivierte Richtlinie aktivieren. Dadurch können beispielsweise strengere Einstellungen des Antiviren-Schutzes bei Virenangriffen festgelegt werden.
- Eine Richtlinie kann untergeordnete Richtlinien haben.

Im Allgemeinen können Sie Richtlinien als Vorbereitung für Notfallsituationen wie Virenangriffe verwenden. Beispiel: Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. In diesem Fall wird die aktuell aktive Richtlinie automatisch inaktiv.

Um zu verhindern, dass mehrere Richtlinien verwaltet werden, können Sie beispielsweise Richtlinienprofile verwenden, wenn bei verschiedenen Gelegenheiten nur bestimmte Einstellungen geändert werden müssen.

Ein *Richtlinienprofil* stellt eine benannte Teilmenge von Einstellungswerten einer Richtlinie dar, welche die Einstellungswerte in einer Richtlinie ersetzen. Ein Richtlinienprofil wirkt sich auf die effektive Formation der Einstellungen auf einem verwalteten Gerät aus. *Effektive Einstellungen* stellen eine Zusammenstellung an Einstellungen für Richtlinien, Richtlinienprofile und lokalen Anwendungseinstellungen dar, die derzeit für das Gerät angewendet werden.

Richtlinienprofile funktionieren entsprechend den folgenden Regeln:

- Ein Richtlinienprofil wird wirksam, wenn eine bestimmte Aktivierungsbedingung auftritt.
- Richtlinienprofile enthalten Werte für Einstellungen, die von den Richtlinieneinstellungen abweichen.
- Durch das Aktivieren eines Richtlinienprofils werden die effektiven Einstellungen des verwalteten Gerätes geändert.
- Eine Richtlinie kann nicht mehr als 100 Richtlinienprofile enthalten.

Über das Schloss und gesperrte Einstellungen

Jede Richtlinieneinstellung verfügt über eine Schaltfläche mit einem Sperren-Symbol (🔒). Die folgende Tabelle zeigt die Statuswerte der Schaltflächen zum Sperren an:

Status der Sperrschaltfläche

Status	Beschreibung
🔒 Nicht definiert	Wenn neben einer Einstellung eine offene Sperre angezeigt wird und die Umschalttaste deaktiviert ist, wird die Einstellung in der Richtlinie nicht angegeben. Ein Benutzer kann diese Einstellungen in der Oberfläche der verwalteten Anwendung ändern. Diese Art von Einstellungen wird als *entsperrt* bezeichnet.
🔒 Erzwingen	Wenn neben einer Einstellung eine Sperre angezeigt wird und die Umschalttaste aktiviert ist, wird die Einstellung auf die Geräte angewendet, auf denen die Richtlinie erzwungen wird. Ein Benutzer kann die Werte dieser Einstellungen in Oberfläche einer verwalteten Anwendung nicht ändern. Diese Art von Einstellungen wird als *gesperrt* bezeichnet.

Es wird dringend empfohlen, dass Sie für Richtlinieneinstellungen, die Sie auf verwalteten Geräten anwenden möchten, die Sperre aktivieren. Nicht gesperrte Richtlinieneinstellungen können in den Einstellungen der Kaspersky-Anwendungen auf verwalteten Geräten geändert werden.

Sie können eine Sperrschaltfläche verwenden, um die folgenden Aktionen auszuführen:

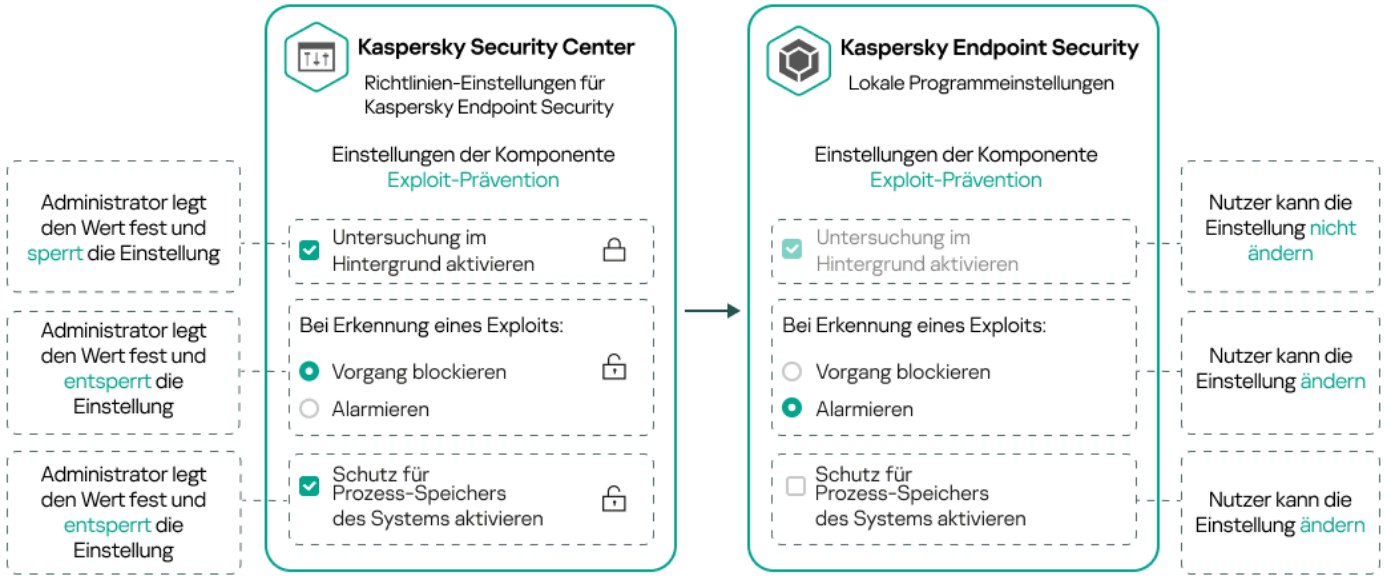
- Sperren von Einstellungen für eine Verwaltungsuntergruppenrichtlinie
- Sperren von Einstellungen einer Kaspersky-Anwendung auf einem verwalteten Gerät

Eine gesperrte Einstellung wird zum Implementieren effektiver Einstellungen auf einem verwalteten Gerät verwendet.

Ein Vorgang zum effektiven Implementieren von Einstellungen umfasst die folgenden Aktionen:

- Das verwaltete Gerät wendet die Einstellungswerte der Kaspersky-Anwendung an.
- Das verwaltete Gerät wendet gesperrte Einstellungswerte einer Richtlinie an.

Eine Richtlinie und eine verwaltete Kaspersky-Anwendung enthalten dieselben Einstellungen. Wenn Sie Richtlinieneinstellungen konfigurieren, ändern die Einstellungen der Kaspersky-Anwendung die Werte auf einem verwalteten Gerät. Sie können gesperrte Einstellungen auf einem verwalteten Gerät nicht anpassen (siehe Abbildung unten):



Sperren und Einstellungen der Kaspersky-Anwendungen

Vererbung von Richtlinien und Richtlinienprofilen

Dieser Abschnitt enthält Informationen zur Hierarchie und Vererbung von Richtlinien und Richtlinienprofilen.

Hierarchie der Richtlinien

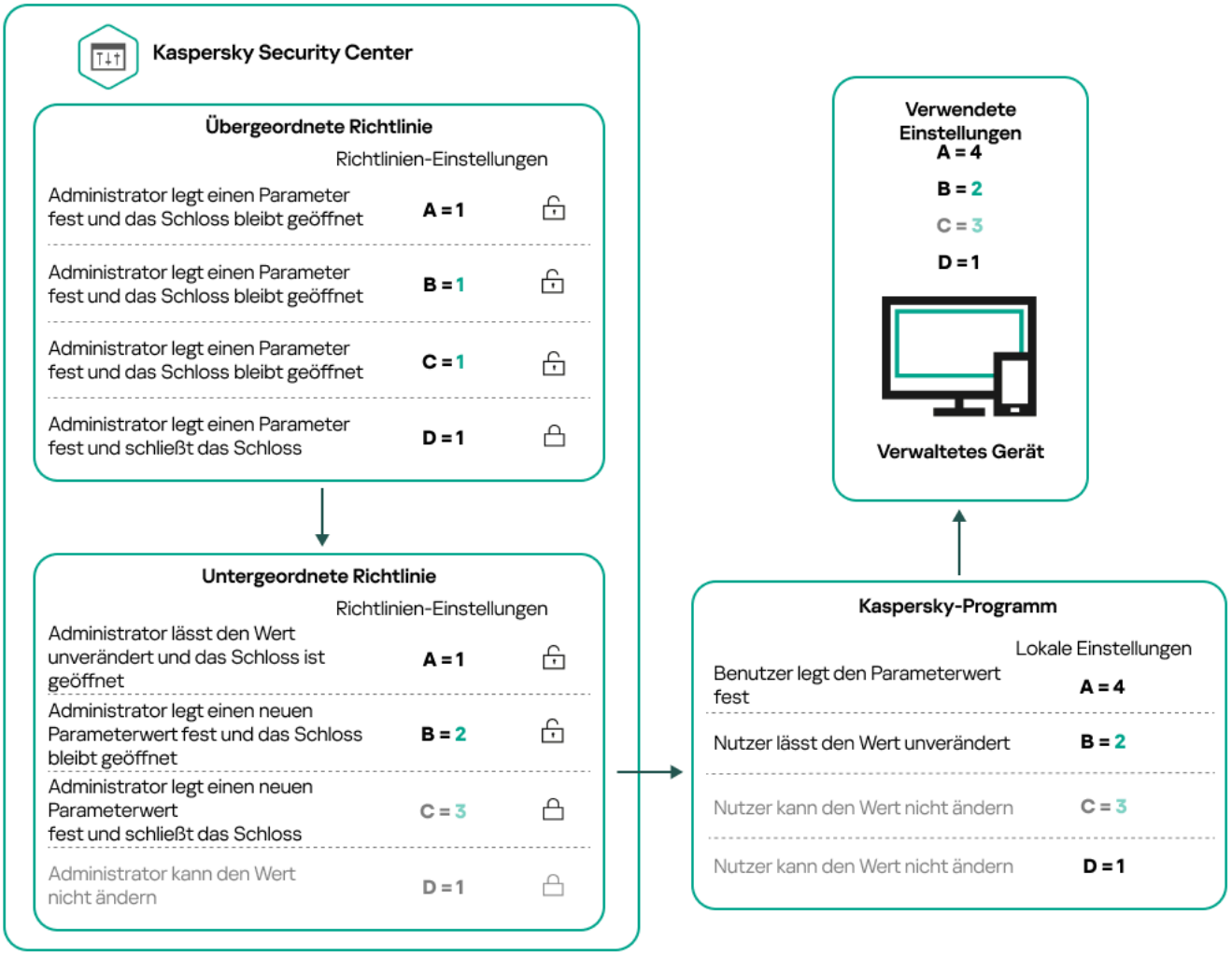
Wenn unterschiedliche Geräte unterschiedliche Einstellungen benötigen, können Sie Geräte in Administrationsgruppen organisieren.

Sie können eine Richtlinie für eine einzelne Administrationsgruppe angeben. Richtlinieneinstellungen können *vererbt* werden. Vererbung bedeutet, dass Richtlinieneinstellungswerte in Untergruppen (untergeordneten Gruppen) von einer Richtlinie einer übergeordneten Administrationsgruppe empfangen werden.

Im Weiteren wird eine Richtlinie für eine übergeordnete Gruppe auch als *übergeordnete Richtlinie* bezeichnet. Eine Richtlinie für eine Untergruppe (untergeordnete Gruppe) wird auch als *untergeordnete Richtlinie* bezeichnet.

Standardmäßig ist auf dem Administrationsserver mindestens eine Gruppe mit verwalteten Geräten vorhanden. Wenn Sie benutzerdefinierte Gruppen erstellen möchten, werden diese als Untergruppen (untergeordnete Gruppen) innerhalb der Gruppe mit verwalteten Geräten erstellt.

Richtlinien derselben Anwendung wirken gemäß einer Hierarchie von Verwaltungsgruppen aufeinander ein. Gesperrte Einstellungen aus einer Richtlinie einer übergeordneten Administrationsgruppe weisen die Richtlinieneinstellungswerte einer Untergruppe neu zu (siehe Abbildung unten).

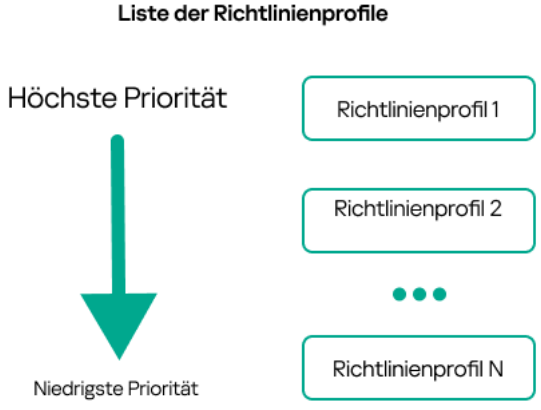


Hierarchie der Richtlinien

Richtlinienprofile in einer Hierarchie von Richtlinien

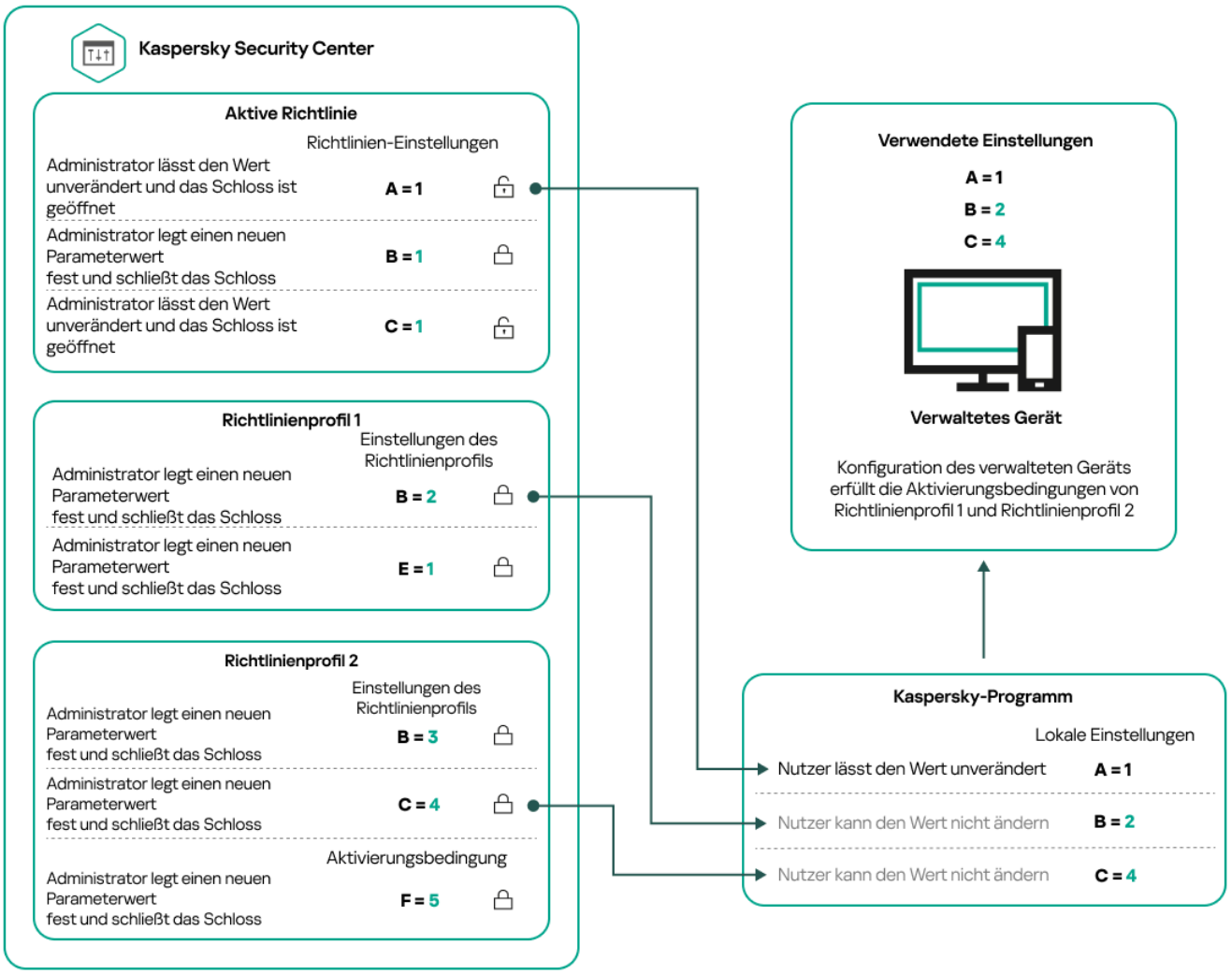
Richtlinienprofile haben die folgenden Bedingungen für die Prioritätszuweisung:

- Die Position eines Profils in einer Richtlinienprofilliste gibt seine Priorität an. Die Priorität eines Richtlinienprofils kann geändert werden. Die höchste Position in einer Liste gibt die höchste Priorität an (siehe Abbildung unten).



Prioritätsdefinition eines Richtlinienprofils

- Die Aktivierungsbedingungen von Richtlinienprofilen hängen nicht voneinander ab. Es können mehrere Richtlinienprofile gleichzeitig aktiviert werden. Wenn sich mehrere Richtlinienprofile auf dieselbe Einstellung auswirken, übernimmt das Gerät den Einstellungswert aus dem Richtlinienprofil mit der höchsten Priorität (siehe Abbildung unten).



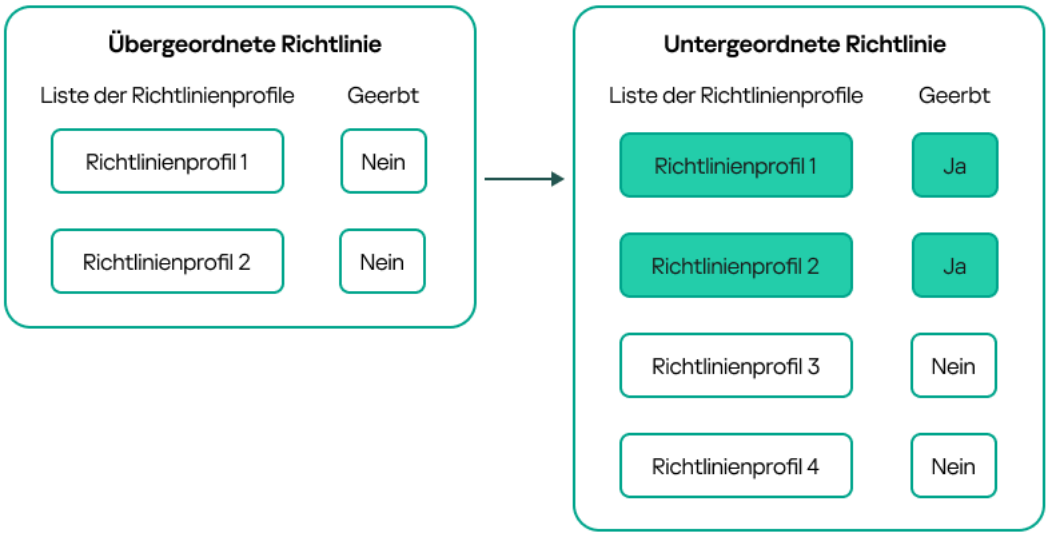
Die Konfiguration des verwalteten Geräts erfüllt die Aktivierungsbedingungen mehrerer Richtlinienprofile.

Richtlinienprofile in einer Vererbungshierarchie

Richtlinienprofile aus verschiedenen Richtlinien auf Hierarchieebene erfüllen die folgenden Bedingungen:

- Eine Richtlinie auf niedrigerer Ebene erbt Richtlinienprofile von einer Richtlinie auf höherer Ebene. Ein Richtlinienprofil, das von einer übergeordneten Richtlinie geerbt wurde, erhält eine höhere Priorität als die Ebene des ursprünglichen Richtlinienprofils.

- Die Priorität eines geerbten Richtlinienprofils kann nicht geändert werden (siehe Abbildung unten).



Vererbung von Richtlinienprofilen

Richtlinienprofile mit demselben Namen

Wenn zwei Richtlinien mit demselben Namen in unterschiedlichen Hierarchieebenen vorhanden sind, funktionieren diese Richtlinien gemäß den folgenden Regeln:

- Gesperrte Einstellungen und die Profilaktivierungsbedingung eines übergeordneten Richtlinienprofils ändern die Einstellungen und die Profilaktivierungsbedingung eines untergeordneten Richtlinienprofils (siehe Abbildung unten).



Das untergeordnete Profil erbt Einstellungswerte von einem übergeordneten Richtlinienprofil.

- Entsperrte Einstellungen und die Profilaktivierungsbedingung eines übergeordneten Richtlinienprofils ändern nicht die Einstellungen und die Profilaktivierungsbedingung eines untergeordneten Richtlinienprofils.

Implementierung der Einstellungen auf einem verwalteten Gerät

Die Implementierung von effektiven Einstellungen auf einem verwalteten Gerät kann wie folgt beschrieben werden:

- Die Werte aller Einstellungen, die nicht gesperrt wurden, werden aus der Richtlinie übernommen.
- Anschließend werden sie mit den Einstellungswerten der verwalteten Anwendung überschrieben.
- Anschließend werden die gesperrten Einstellungswerte aus der effektiven Richtlinie angewendet. Die Werte gesperrter Einstellungen ändern die Werte nicht gesperrter effektiver Einstellungen.

Richtlinien verwalten

Dieser Abschnitt beschreibt das Verwalten von Richtlinien und enthält Informationen zum Anzeigen der Richtlinienliste, zum Erstellen einer Richtlinie, zum Ändern einer Richtlinie, zum Kopieren einer Richtlinie, zum Verschieben einer Richtlinie, zum erzwungenen Synchronisieren, zum Anzeigen des Statusdiagramms für die Richtlinienverteilung und zum Löschen einer Richtlinie.

Richtlinienliste anzeigen

Sie können die Richtlinienlisten für den Administrationsserver oder für jede beliebige Administrationsgruppe anzeigen.

Um sich die Richtlinienliste anzeigen zu lassen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.

2. Wählen Sie in der Struktur der Administrationsgruppe die Administrationsgruppe aus, für welche Sie die Liste mit Richtlinien anzeigen möchten.

   Daraufhin wird die Liste der Richtlinien in Tabellenformat geöffnet. Wenn noch keine Richtlinien existieren, ist die Tabelle leer. Sie können die Spalten der Tabelle ein- und ausblenden, ihre Reihenfolge verändern, nur Zeilen mit einem bestimmten Wert anzeigen und die Suchfunktion verwenden.

Richtlinie erstellen

Sie können Richtlinien erstellen sowie Sie bestehende Richtlinien ändern und löschen.

Um eine Richtlinie zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

2. Wählen Sie die Administrationsgruppe aus, für welche die Richtlinie erstellt werden soll:

   - Für die Stammgruppe:

     In diesem Fall können Sie mit dem nächsten Schritt fortfahren.

   - Für eine untergeordnete Gruppe:

     a. Klicken Sie im oberen Bereich des Fensters auf den Link mit dem aktuellen Pfad.

     b. Klicken Sie im neuen Fenster auf den Link mit dem Namen der erforderlichen Untergruppe.

     Der aktuelle Pfad ändert sich entsprechend der ausgewählten untergeordneten Gruppe.

3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Programm auswählen** wird geöffnet.

4. Wählen Sie die Anwendung aus, für das Sie eine Richtlinie erstellen möchten.

5. Klicken Sie auf die Schaltfläche **Weiter**.

   Das Fenster für neue Richtlinieneinstellungen wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.

6. Ändern Sie gegebenenfalls Standardname, Standardstatus und Standardvererbungseinstellungen der Richtlinie.

7. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

   Sie können aber auch auf **Speichern** klicken und beenden. Die Richtlinie wird in der Liste der Richtlinien angezeigt, und Sie können ihre Einstellungen später anpassen.

8. Wählen Sie auf der Registerkarte **Programmeinstellungen** im linken Bereich die gewünschte Kategorie aus und ändern Sie im Ergebnisbereich auf der rechten Seite die Einstellungen der Richtlinie. Sie können die Einstellungen der Richtlinie in jeder Kategorie (jedem Abschnitt) ändern.

   Der Satz der Einstellungen ist davon abhängig, für welche Anwendung Sie eine Richtlinie erstellen. Weitere Informationen finden Sie hier:

   - Administrationsserver-Konfiguration
   - Richtlinieneinstellungen des Administrationsagenten
   - Dokumentation zu Kaspersky Endpoint Security für Windows

   Ausführliche Informationen über die Einstellungen anderer Sicherheitsanwendungen finden Sie in der Dokumentation der entsprechenden Anwendung.

   Beim Ändern der Einstellungen können Sie auf **Abbrechen** klicken, um den letzten Vorgang rückgängig zu machen.

9. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Die Richtlinie wird in der Liste der Richtlinien angezeigt.

Richtlinie ändern

Um eine Richtlinie zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

2. Klicken Sie auf die Richtlinie, die Sie ändern möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.

3. Geben Sie die Allgemeinen Einstellungen und Einstellungen der Anwendung an, für welches Sie eine Richtlinie erstellen. Weitere Informationen finden Sie hier:

   - Administrationsserver-Konfiguration
   - Richtlinieneinstellungen des Administrationsagenten
   - Dokumentation zu Kaspersky Endpoint Security für Windows

Ausführliche Informationen über die Einstellungen anderer Sicherheitsanwendungen finden Sie in der Dokumentation zu dieser Anwendung.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Änderungen der Richtlinie werden in den Eigenschaften der Richtlinie gespeichert und im Abschnitt **Revisionsverlauf** angezeigt.

Allgemeine Richtlinieneinstellungen

Allgemein

Auf der Registerkarte **Allgemein** können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:
  - **Aktiv**

    Bei Auswahl dieser Option wird die Richtlinie aktiv.

    Diese Variante ist standardmäßig ausgewählt.
  - **Mobil**

    Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.
  - **Inaktiv**

    Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.
- In der Einstellungsgruppe **Einstellungen erben** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:
  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.
  - **Vererbung der Einstellungen an untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:
    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.
    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

    Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Auf der Registerkarte **Konfiguration von Ereignissen** können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Die Ereignisse werden anhand der Ereigniskategorie auf folgende Registerkarten aufgeteilt:

- **Kritisch**

  Der Abschnitt **Kritisch** wird in den Eigenschaften der Richtlinie des Administrationsagenten nicht angezeigt.

- **Funktionsfehler**
- **Warnung**
- **Information**

Jeder Abschnitt enthält eine Liste mit Ereignistypen und der Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen). Mit einem Klick auf einen Ereignistyp können Sie die folgenden Einstellungen festlegen:

- **Ereignisregistrierung**

  Sie können angeben, wie viele Tage und an welchem Ort das Ereignis gespeichert werden soll:

  - **Mittels Syslog in ein SIEM-System exportieren**
  - **Im System-Ereignisprotokoll des Geräts speichern**
  - **Im System-Ereignisprotokoll des Administrationsservers speichern**

- **Ereignisbenachrichtigungen**

  Sie können bestimmen, ob Sie auf eine der folgenden Arten über das Ereignis benachrichtigt werden möchten:

  - **Per E-Mail benachrichtigen**
  - **Per SMS benachrichtigen**
  - **Durch den Start einer ausführbaren Datei oder eines Skriptes benachrichtigen**
  - **Per SNMP benachrichtigen**

  Standardmäßig werden die Benachrichtigungseinstellungen verwendet, die auf der Registerkarte "Eigenschaften des Administrationsservers" angegeben sind (z. B. Empfängeradresse). Wenn Sie möchten, können Sie diese Einstellungen auf den Registerkarten **E-Mail**, **SMS** und **Start einer ausführbaren Datei** ändern.

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie eine Liste mit Revisionen der Richtlinie anzeigen und bei Bedarf ein Rollback der Änderungen an der Richtlinie vornehmen.

Option zur Vererbung einer Richtlinie aktivieren und deaktivieren

So aktivieren oder deaktivieren Sie die Vererbungsoption in einer Richtlinie:

1. Öffnen Sie die erforderliche Richtlinie.
2. Öffnen Sie die Registerkarte **Allgemein**.
3. Aktivieren oder Deaktivieren der Richtlinienvererbung:
   - Wenn Sie **Einstellungen aus übergeordneter Richtlinie erben** in einer untergeordneten Richtlinie aktivieren und ein Administrator einige Einstellungen in der übergeordneten Richtlinie sperrt, können Sie diese Einstellungen in der untergeordneten Richtlinie nicht ändern.
   - Wenn Sie die Option **Einstellungen aus übergeordneter Richtlinie erben** für eine untergeordnete Gruppe deaktivieren, können Sie alle Einstellungen in der untergeordneten Gruppe bearbeiten, selbst wenn einige Einstellungen in der übergeordneten Richtlinie mit einem Schloss gesperrt sind.
   - Wenn Sie **Vererbung der Einstellungen an untergeordnete Richtlinien erzwingen** in der übergeordneten Gruppe aktivieren, wird dadurch **Einstellungen aus übergeordneter Richtlinie erben** für alle untergeordneten Richtlinien aktiviert. In diesem Fall kann diese Option nicht für untergeordnete Richtlinien deaktiviert werden. Alle Einstellungen, die in der übergeordneten Richtlinie gesperrt sind, werden zwangsweise an untergeordnete Gruppen vererbt und können in den untergeordneten Gruppen nicht bearbeitet werden.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Abbrechen**, um sie zu verwerfen.

Standardmäßig ist die Option **Einstellungen aus übergeordneter Richtlinie erben** für eine neue Richtlinie aktiviert.

Wenn eine Richtlinie über Profile verfügt, erben alle untergeordneten Richtlinien diese Profile.

Richtlinien kopieren

Richtlinien können von einer Administrationsgruppe zu einer anderen kopiert werden.

Um eine Richtlinie zu einer anderen Administrationsgruppe zu kopieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie (oder den Richtlinien), die Sie kopieren möchten.
3. Klicken Sie auf die Schaltfläche **Kopieren**.

   Im rechten Bereich des Bildschirms erscheint die Strukturansicht der Administrationsgruppen.
4. Wählen Sie in der Strukturansicht die Zielgruppe aus. Das ist die Gruppe, zu der Sie die Richtlinie (oder die Richtlinien) kopieren möchten.
5. Klicken Sie auf die Schaltfläche **Kopieren** am unteren Rand des Bildschirms.
6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Die Richtlinie bzw. Richtlinien werden samt allen Profilen zur Zielgruppe kopiert. Der Status jeder kopierten Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

Wenn die gewählte Richtlinienliste bereits eine Richtlinie mit dem gleichen Namen wie die zu verschiebende Richtlinie enthält, wird dem Namen der verschobenen Richtlinie eine Endung der Form (<laufende Nummer>) angehängt. Beispiel: (1).

Richtlinie verschieben

Richtlinien können von einer Administrationsgruppe zu einer anderen verschoben werden. Angenommen, Sie möchten eine Gruppe löschen, aber ihre Richtlinien für eine andere Gruppe verwenden. In diesem Fall können Sie die Richtlinie der alten Gruppe zur neuen Gruppe verschieben, bevor Sie die Gruppe löschen.

Beim Verschieben einer Richtlinie in eine andere Verwaltungsgruppe wird der Revisionsverlauf der Richtlinie gelöscht. Auf der Registerkarte **Revisionsverlauf** werden nur Informationen zur letzten Änderung angezeigt.

Um eine Richtlinie zu einer anderen Administrationsgruppe zu verschieben, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie (oder den Richtlinien), die Sie verschieben möchten.
3. Klicken Sie auf die Schaltfläche **Verschieben**.

   Im rechten Bereich des Bildschirms erscheint die Strukturansicht der Administrationsgruppen.
4. Wählen Sie in der Strukturansicht die Zielgruppe aus. Das ist die Gruppe, zu der Sie die Richtlinie (oder die Richtlinien) verschieben möchten.
5. Klicken Sie auf die Schaltfläche **Verschieben** am unteren Rand des Bildschirms.
6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

   Wenn die Richtlinie nicht von der Quellgruppe geerbt wurde, wird sie samt allen Profilen zur Zielgruppe verschoben. Der Status der Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

   Wenn die Richtlinie von der Quellgruppe geerbt wurde, bleibt sie in der Quellgruppe erhalten. Sie wird samt allen Profilen zur Zielgruppe kopiert. Der Status der Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

Wenn die gewählte Richtlinienliste bereits eine Richtlinie mit dem gleichen Namen wie die zu verschiebende Richtlinie enthält, wird dem Namen der verschobenen Richtlinie eine Endung der Form (<laufende Nummer>) angehängt. Beispiel: (1).

Richtlinien exportieren

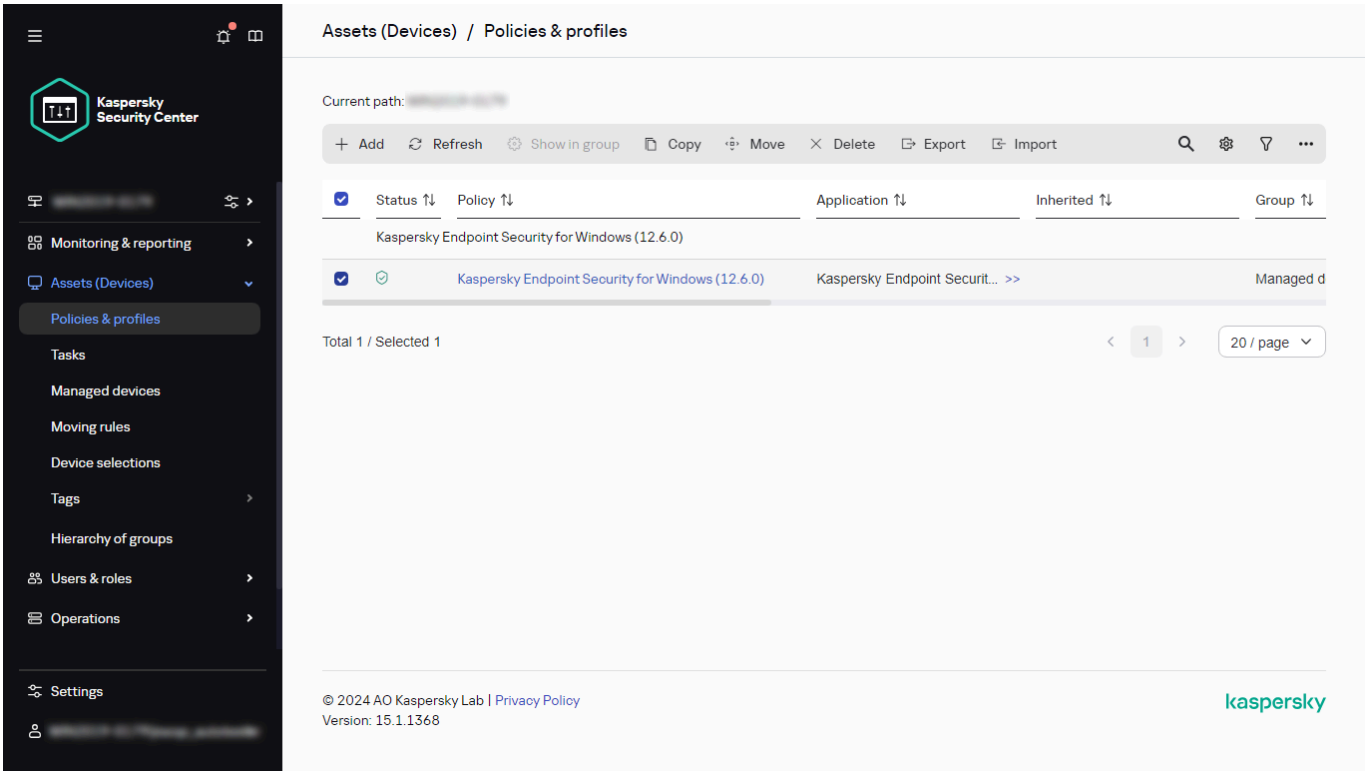
Mit Kaspersky Security Center können Sie eine Richtlinie, deren Einstellungen und Richtlinienprofile in einer klp-Datei speichern. Sie können diese klp-Datei verwenden, um sowohl in Kaspersky Security Center Windows als auch in Kaspersky Security Center Linux die gespeicherte Richtlinie zu importieren.

Um eine Richtlinie zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

2. Aktivieren Sie das Kontrollkästchen neben der Richtlinie, die Sie installieren möchten.

   Sie können nicht mehrere Richtlinien gleichzeitig exportieren. Wenn Sie mehr als eine Richtlinie auswählen, wird die Schaltfläche **Exportieren** deaktiviert.



3. Klicken Sie auf die Schaltfläche **Exportieren**.

4. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Richtliniendatei an. Klicken Sie auf **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Richtliniendatei automatisch im Ordner **Downloads** gespeichert.

Richtlinien importieren

Mit Kaspersky Security Center können Sie eine Richtlinie aus einer klp-Datei importieren. Die klp-Datei enthält die exportierte Richtlinie, deren Einstellungen und Richtlinienprofile.

So importieren Sie eine Richtlinie:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

2. Klicken Sie auf die Schaltfläche **Importieren**.

3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Richtliniendatei auszuwählen, die Sie importieren möchten.

4. Geben Sie im folgenden Fenster den Pfad zur klp-Richtliniendatei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Richtliniendatei auswählen können.

   Die Verarbeitung der Richtlinien beginnt.

5. Nachdem die Richtlinie erfolgreich verarbeitet wurde, wählen Sie die Administrationsgruppe aus, auf die Sie die Richtlinie anwenden möchten.

6. Klicken Sie auf die Schaltfläche **Abgeschlossen**, um den Import der Richtlinie abzuschließen.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Richtlinie erfolgreich importiert wurde, können Sie zum Anzeigen der Eigenschaften der Richtlinie auf den Link **Details** klicken.

Nach einem erfolgreichen Import wird die Richtlinie in der Liste der Richtlinien angezeigt. Die Einstellungen und Profile der Richtlinie werden ebenfalls importiert. Unabhängig vom Richtlinienstatus, der während des Exports ausgewählt wurde, ist die importierte Richtlinie inaktiv. Sie können den Richtlinienstatus in den Eigenschaften der Richtlinie ändern.

Wenn die neu importierte Richtlinie denselben Namen wie eine bereits vorhandene Richtlinie besitzt, wird der Name der importierten Richtlinie um den Index **(<nächste Sequenznummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Anzeigen des Statusdiagramms für die Richtlinienverteilung

In Kaspersky Security Center können Sie den Übernahmestatus einer Richtlinie für jedes Gerät in einem Statusdiagramm zur Richtlinienverteilung anzeigen.

Um das Statusdiagramm für die Richtlinienverteilung für jedes Gerät anzuzeigen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

2. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, für die Sie den Verteilungsstatus auf dem Gerät anzeigen wollen.

3. Wählen Sie im sich öffnenden Menü den Link **Verteilung**.

   Das Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird geöffnet.

4. Im geöffneten Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird eine **Statusbeschreibung** der Richtlinie angezeigt.

Sie können die Anzahl der angezeigten Ergebnisse in der Liste der Richtlinienverteilung ändern. Die maximale Anzahl an Geräten ist 100.000.

Um die Anzahl der in der Liste mit den Ergebnissen der Richtlinienverteilung angezeigten Geräte zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Einstellungen der Benutzeroberfläche.**

2. Geben Sie für **Obergrenze der in den Ergebnissen der Richtlinienverteilung angezeigten Geräte** die Anzahl an Geräten ein (bis zu 100.000).

   Die standardmäßige Anzahl beträgt 5000.

3. Klicken Sie auf die Schaltfläche **Speichern**.

   Ihre Einstellungen werden gespeichert und übernommen.

Richtlinien löschen

Eine nicht mehr benötigte Richtlinie kann gelöscht werden. Sie können nur Richtlinien löschen, die in der angegebenen Administrationsgruppe nicht geerbt sind. Eine geerbte Richtlinie kann nur in der Gruppe der höheren Ebene gelöscht werden, für die sie erstellt wurde.

Um eine Richtlinie zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie, die Sie löschen möchten, und klicken Sie auf **Löschen**.

   Die Schaltfläche **Löschen** ist nicht verfügbar (abgeblendet), wenn Sie eine geerbte Richtlinie auswählen.
3. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Die Richtlinie wird samt allen Profilen gelöscht.

Richtlinienprofile verwalten

Dieser Abschnitt beschreibt die Verwaltung von Richtlinienprofilen und enthält Informationen zum Anzeigen der Profile einer Richtlinie, zum Ändern einer Richtlinienprofilpriorität, zum Erstellen eines Richtlinienprofils, zum Ändern eines Richtlinienprofils, zum Kopieren eines Richtlinienprofils, zum Erstellen einer Richtlinienprofilaktivierungsregel und zum Löschen eines Richtlinienprofils.

Profile einer Richtlinie anzeigen

So zeigen Sie Profile einer Richtlinie an:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf den Namen der Richtlinie, deren Profile Sie anzeigen möchten.

   Das Fenster mit den Eigenschaften der Richtlinie wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.
3. Öffnen Sie die Registerkarte **Richtlinienprofile**.

Daraufhin wird die Liste der Richtlinienprofile in Tabellenformat geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

Priorität eines Richtlinienprofils ändern

Um die Priorität eines Richtlinienprofils zu ändern, gehen Sie wie folgt vor:

1. Gehen Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Aktivieren Sie auf der Registerkarte **Richtlinienprofile** das Kontrollkästchen neben dem Richtlinienprofil, dessen Priorität Sie ändern möchten.

3. Ändern Sie die Position des Richtlinienprofils in der Liste, indem Sie auf **Priorisieren** oder **Priorisierung verringern** klicken.

   Je höher ein Richtlinienprofil in der Liste steht, desto höher ist seine Priorität.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Priorität des ausgewählten Richtlinienprofils wird verändert und angewendet.

Richtlinienprofil erstellen

Um ein Richtlinienprofil zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Ändern Sie gegebenenfalls den Standardnamen und die Standardvererbungseinstellungen des Profils.

4. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

   Alternativ dazu können Sie auf **Speichern** klicken und beenden. Das Profil, das Sie erstellt haben, wird in der Liste der Richtlinienprofile angezeigt, und Sie können seine Einstellungen später anpassen.

5. Wählen Sie auf der Registerkarte **Programmeinstellungen** im linken Bereich die gewünschte Kategorie aus und ändern Sie im Ergebnisbereich auf der rechten Seite die Einstellungen für das Profil. Sie können die Einstellungen des Richtlinienprofils in jeder Kategorie (jedem Abschnitt) ändern.

   Beim Ändern der Einstellungen können Sie auf **Abbrechen** klicken, um den letzten Vorgang rückgängig zu machen.

6. Klicken Sie auf **Speichern**, um das Profil zu speichern.

Das Profil wird in der Liste der Richtlinienprofile angezeigt.

Richtlinienprofil ändern

Richtlinienprofile können nur für Richtlinien von Kaspersky Endpoint Security für Windows geändert werden.

Um die Einstellungen eines Richtlinienprofils zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, das Sie bearbeiten möchten.

   Daraufhin wird das Eigenschaftenfenster des Richtlinienprofils geöffnet.

3. Passen Sie im Eigenschaftenfenster die Einstellungen des Profils an:

   - Ändern Sie auf der Registerkarte **Allgemein** bei Bedarf den Namen des Profils und aktivieren bzw. deaktivieren Sie das Profil.
   - Bearbeiten Sie die Regeln für die Profilaktivierung.
   - Programmeinstellungen bearbeiten.

   Ausführliche Informationen über die Einstellungen von Sicherheitsanwendungen finden Sie in der Dokumentation der entsprechenden Anwendung.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die geänderten Einstellungen werden nach der Synchronisierung des Geräts mit dem Administrationsserver (wenn das Richtlinienprofil aktiv ist) bzw. nach der Ausführung der Aktivierungsregeln (wenn das Richtlinienprofil nicht aktiv ist) angewendet.

Richtlinienprofil kopieren

Sie können ein Richtlinienprofil zur aktuellen oder zu einer anderen Richtlinie kopieren, wenn Sie z. B. identische Profile für verschiedene Richtlinien festlegen möchten. Das Kopieren von Profilen ist auch dann nützlich, wenn Sie zwei oder mehrere Profile anlegen möchten, deren Einstellungen sich nur minimal unterscheiden.

Um ein Richtlinienprofil zu kopieren, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, das Sie kopieren möchten.
3. Klicken Sie auf die Schaltfläche **Kopieren**.
4. Wählen Sie im nächsten Fenster die Richtlinie aus, zu der Sie das Profil kopieren möchten.

   Das Richtlinienprofil kann zur gleichen Richtlinie oder zu einer von Ihnen angegebenen Richtlinie kopiert werden.

5. Klicken Sie auf die Schaltfläche **Kopieren**.

Das Richtlinienprofil wird zur festgelegten Richtlinie kopiert. Dem zuletzt kopierten Profil wird die niedrigste Priorität zugewiesen. Wenn Sie das Profil zur selben Richtlinie kopieren, wird dem neu kopierten Profil der Index () angehängt, z. B. (1), (2).

Die Einstellungen des Profils, einschließlich Name und Priorität, können später geändert werden; das ursprüngliche Richtlinienprofil ändert sich in diesem Fall nicht.

Regeln für die Aktivierung des Richtlinienprofils erstellen

Um eine Regel für die Aktivierung des Richtlinienprofils zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, für das Sie eine Aktivierungsregel anlegen möchten.

   Wenn die Richtlinienprofilliste leer ist, können Sie ein Richtlinienprofil erstellen.

3. Klicken Sie auf der Registerkarte **Aktivierungsregeln** auf die Schaltfläche **Hinzufügen**.

   Das Fenster mit Regeln für die Aktivierung des Richtlinienprofils wird geöffnet.

4. Geben Sie einen Namen für die Regel ein.

5. Aktivieren Sie die Kontrollkästchen neben den Bedingungen, die Einfluss auf die Aktivierung des erstellten Richtlinienprofils haben sollen:

   - **Allgemeine Regeln für die Aktivierung des Richtlinienprofils**

     Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät je nach dem Zustand des autonomen Modus des Geräts, der Verbindungsregel des Geräts mit dem Administrationsserver und den dem Gerät zugewiesenen Tags anzupassen.

     Geben Sie für diese Option im nächsten Schritt Folgendes an:

     - **Gerätestatus**

       Legt die Bedingung für die Verfügbarkeit des Geräts im Netzwerk fest:

       - **Online** – Das Gerät befindet sich im Netzwerk und somit ist der Administrationsserver ist verfügbar.
       - **Autonom** – Das Gerät befindet sich in einem externen Netzwerk, daher ist der Administrationsserver nicht verfügbar.
       - **N/A** – Das Kriterium wird nicht angewendet.

     - **Die Regel für die Verbindung des Administrationsservers ist auf diesem Gerät aktiv**

       Wählen Sie die Aktivierungsbedingung für das Richtlinienprofil (Regel wird erfüllt bzw. nicht erfüllt) und bestimmen Sie den Regelnamen.

       Die Regel definiert den Netzwerkstandort des Geräts für die Verbindung mit dem Administrationsserver; bei Erfüllen bzw. Nichterfüllen ihrer Bedingungen wird das Richtlinienprofil aktiviert.

       Die Beschreibung des Netzwerkstandorts der Geräte für die Verbindung mit dem Administrationsserver kann erstellt oder in der Regel für die Umschaltung des Administrationsagenten angepasst werden.

   - **Regeln für einen bestimmten Gerätebesitzer**

     Geben Sie für diese Option im nächsten Schritt Folgendes an:

     - **Gerätebesitzer**

       Aktivieren Sie die Option, um die Aktivierungsregel des Profils auf dem Gerät anhand des Geräteinhabers anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

       - Gerät gehört dem angegebenen Inhaber ("="-Symbol).
       - Gerät gehört nicht dem angegebenen Inhaber ("#"-Symbol).

         Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können den Gerätebesitzer angeben, wenn die Option aktiviert ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Gerätebesitzer gehört zu einer internen Sicherheitsgruppe**

  Aktivieren Sie die Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Zugehörigkeit des Geräteinhabers zur internen Sicherheitsgruppe von Kaspersky Security Center anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

  - Der Gerätebesitzer gehört zur angegebenen Sicherheitsgruppe ("="-Symbol).
  - Der Gerätebesitzer gehört nicht zur angegebenen Sicherheitsgruppe ("#"-Symbol).

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können eine Sicherheitsgruppe von Kaspersky Security Center angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Regeln für Hardware-Eigenschaften**

  Aktivieren Sie das Kontrollkästchen, um auf dem Gerät die Aktivierung der Richtlinienprofile je nach Speichergröße und Anzahl seiner logischen Prozesse anzupassen.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Arbeitsspeichergröße (MB)**

    Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Arbeitsspeichergröße des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

    - Arbeitsspeicher des Geräts kleiner als festgelegter Wert (Zeichen "<")
    - Arbeitsspeicher des Geräts größer als festgelegter Wert (Zeichen ">")

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Größe des Arbeitsspeichers auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

  - **Anzahl der logischen Prozessoren**

    Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Anzahl der logischen Prozessoren des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

    - Anzahl der logischen Prozesse des Geräts kleiner oder gleich festgelegter Wert (Zeichen "<")
    - Anzahl der logischen Prozesse des Geräts größer oder gleich festgelegter Wert (Zeichen ">")

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Anzahl der logischen Prozessoren auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Regeln für Rollenzuordnung**

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  Richtlinienprofil durch eine bestimmte Rolle des Gerätebesitzers aktivieren

  Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät in Abhängigkeit von der Rolle des Besitzers zu konfigurieren. Fügen Sie die Rolle manuell aus der Liste vorhandener Rollen hinzu.

Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt.

- **Regeln für die Verwendung von Tags**

  Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät abhängig von den Tags anzupassen, die dem Gerät zugewiesen wurden. Sie können das Richtlinienprofil entweder für alle Geräte mit diesem Tag oder alle Geräte ohne dieses Tag aktivieren.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Tag**

    Geben Sie in der Liste der Tags Aktivierungsregeln für Geräte im Richtlinienprofil an, indem Sie die Kontrollkästchen der entsprechenden Tags aktivieren.

    Sie können neue Tags zur Liste hinzufügen, indem Sie diese im Feld über der Liste eingeben und auf die Schaltfläche **Hinzufügen** klicken.

    Das Richtlinienprofil erstreckt sich auf Geräte, in deren Beschreibung alle ausgewählten Tags vorkommen. Sind Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt. Standardmäßig sind die Kontrollkästchen deaktiviert.

  - **Auf Geräte ohne angegebene Tags anwenden**

    Aktivieren Sie die Option, wenn die Auswahl der Tags invertiert werden muss.

    Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in das Richtlinienprofil aufgenommen. Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

    Diese Option ist standardmäßig deaktiviert.

- **Regeln für die Verwendung von Active Directory**

  Aktivieren Sie dieses Kontrollkästchen, um die Aktivierungsregeln für das Richtlinienprofil auf dem Gerät anzupassen. Die Regeln sind davon abhängig, ob das Gerät in einer Active Directory-Organisationseinheit (OU) vorhanden ist oder ob das Gerät (oder dessen Eigentümer) zu einer Active Directory-Sicherheitsgruppe gehört.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Zugehörigkeit des Gerätebesitzers zu einer Active Directory-Sicherheitsgruppe**

    Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert, wenn dessen Inhaber Mitglied der angegebenen Sicherheitsgruppe ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

  - **Zugehörigkeit des Geräts zur Sicherheitsgruppe Active Directory**

    Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

  - **Gerätezuordnung in der Active Directory-Organisationseinheit**

    Bei aktivierter Option wird das Richtlinienprofil auf einem Gerät aktiviert, das explizit oder implizit in der angegebenen Active Directory-Organisationseinheit (OU) enthalten ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt.

    Diese Option ist standardmäßig deaktiviert.

Von der Auswahl der Einstellungen im ersten Schritt hängt die weitere Anzahl der Seiten des Assistenten ab. Sie können die Regeln für die Richtlinienprofilaktivierung später ändern.

6. Überprüfen Sie die Liste der angepassten Einstellungen. Ist die Liste korrekt, klicken Sie auf **Erstellen**.

   Das Profil wird gespeichert. Das Profil wird auf dem Gerät aktiviert, wenn die Aktivierungsregel ausgeführt wird.

Die Regeln für die Aktivierung des Richtlinienprofils, die für das Profil erstellt wurden, werden in den Eigenschaften des Richtlinienprofils auf der Registerkarte **Aktivierungsregeln** angezeigt. Sie können die Regel für die Aktivierung des Richtlinienprofils ändern oder löschen.

Mehrere Aktivierungsregeln können gleichzeitig ausgeführt werden.

Richtlinienprofil löschen

Um ein Richtlinienprofil zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Aktivieren Sie auf der Registerkarte **Richtlinienprofile** das Kontrollkästchen neben dem Richtlinienprofil, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

3. Klicken Sie im folgenden Fenster erneut auf **Löschen**.

   Das Richtlinienprofil wird gelöscht. Wenn die Richtlinie von einer Gruppe einer niedrigeren Ebene geerbt wird, verbleibt das Profil in dieser Gruppe, wird aber zum Richtlinienprofil dieser Gruppe. Auf diese Weise werden wesentliche Veränderungen an den Einstellungen der verwalteten Anwendungen, die auf Geräten untergeordneter Gruppen installiert sind, unterbunden.

Verschlüsselung und Datenschutz

Die Datenverschlüsselung senkt das Risiko eines unbeabsichtigten Informationsverlustes im Falle des Diebstahls oder Verlustes Ihres Laptops oder Ihrer Festplatte, sowie beim Zugriff nicht autorisierter Benutzer und Programme auf Daten.

Die folgenden Kaspersky-Anwendungen unterstützten Verschlüsselung:

- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security for Mac

Mithilfe der Einstellungen der Benutzeroberfläche können Sie einige von den Elementen der Oberfläche, die sich auf die Funktion der Verschlüsselungsverwaltung beziehen, ein- und ausblenden.

Es wird nicht empfohlen, die Verschlüsselung in einer VDI-Umgebung zu aktivieren.

Verschlüsselung von Daten in Kaspersky Endpoint Security für Windows

Sie können die folgenden Verschlüsselungsarten verwalten:

- BitLocker-Laufwerkverschlüsselung auf Geräten, auf denen ein Windows-Betriebssystem für Server ausgeführt wird
- Kaspersky-Festplattenverschlüsselung auf Geräten mit einem Windows-Betriebssystem für Workstations

Durch die Verwendung dieser Komponenten von Kaspersky Endpoint Security für Windows können Sie beispielsweise die Verschlüsselung aktivieren oder deaktivieren, die Liste der verschlüsselten Laufwerke anzeigen oder Berichte über die Verschlüsselung erstellen und anzeigen.

Sie konfigurieren die Verschlüsselung, indem Sie Richtlinien von Kaspersky Endpoint Security für Windows in Kaspersky Security Center definieren. Kaspersky Endpoint Security für Windows führt die Verschlüsselung und Entschlüsselung gemäß der aktiven Richtlinie aus. Ausführliche Anweisungen zur Konfiguration von Regeln und eine Beschreibung der Verschlüsselungsfunktionen können Sie der Hilfe von Kaspersky Endpoint Security für Windows entnehmen.

Verschlüsselung von Daten in Kaspersky Endpoint Security for Mac

Auf macOS-Geräten können Sie die FileVault-Verschlüsselung verwenden. Während Sie mit Kaspersky Endpoint Security for Mac arbeiten, können Sie diese Verschlüsselung aktivieren oder deaktivieren.

Sie konfigurieren die Verschlüsselung, indem Sie Richtlinien von Kaspersky Endpoint Security for Mac in Kaspersky Security Center definieren. Kaspersky Endpoint Security for Mac führt die Verschlüsselung und Entschlüsselung gemäß der aktiven Richtlinie aus. Eine ausführliche Beschreibung der Verschlüsselungsfunktionen finden Sie in der Hilfe von Kaspersky Endpoint Security for Mac.

Liste der verschlüsselten Laufwerke anzeigen

In Kaspersky Security Center können Sie Details zu verschlüsselten Laufwerken und Geräten, die auf Laufwerksebene verschlüsselt sind, anzeigen. Wenn die Informationen auf einem Laufwerk entschlüsselt wurden, wird das Laufwerk automatisch aus der Liste entfernt.

Um die Liste der verschlüsselten Laufwerke anzuzeigen:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Laufwerke**.

Wenn sich der Abschnitt nicht im Menü befindet, bedeutet dies, dass er ausgeblendet ist. Aktivieren Sie in den Einstellungen der Benutzeroberfläche die Option **Verschlüsselung und Datenschutz anzeigen**, um den Abschnitt anzuzeigen.

Sie können die Liste der verschlüsselten Laufwerke als csv- oder txt-Datei exportieren. Klicken Sie dazu entweder auf **In csv-Datei exportieren** oder auf **In txt-Datei exportieren**.

Liste der Verschlüsselungsereignisse anzeigen

Bei der Ausführung der Aufgaben zur Datenverschlüsselung oder -entschlüsselung auf den Client-Geräten sendet Kaspersky Endpoint Security für Windows an Kaspersky Security Center Informationen über aufgetretene Ereignisse folgender Typen:

- Aufgrund unzureichenden Speicherplatzes kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Aufgrund eines Lizenzproblems kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Aufgrund fehlender Zugriffsrechte kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Das Zugreifen einer Anwendung auf eine verschlüsselte Datei wurde verweigert.
- Unbekannte Fehler.

Um sich eine Liste der Ereignisse anzeigen zu lassen, die bei einer Datenverschlüsselung auf Geräten aufgetreten sind, gehen Sie wie folgt vor:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselungsereignisse**.

Wenn sich der Abschnitt nicht im Menü befindet, bedeutet dies, dass er ausgeblendet ist. Aktivieren Sie in den Einstellungen der Benutzeroberfläche die Option **Verschlüsselung und Datenschutz anzeigen**, um den Abschnitt anzuzeigen.

Sie können die Liste der verschlüsselten Laufwerke als csv- oder txt-Datei exportieren. Klicken Sie dazu entweder auf **In csv-Datei exportieren** oder auf **In txt-Datei exportieren**.

Alternativ können Sie die Liste der Verschlüsselungsereignisse für jedes verwaltete Gerät überprüfen.

So zeigen Sie die Verschlüsselungsereignisse eines verwalteten Geräts an:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen eines verwalteten Geräts.
3. Gehen Sie auf der Registerkarte **Allgemein** zum Abschnitt **Schutz**.
4. Klicken Sie auf den Link **Fehler der Datenverschlüsselung anzeigen**.

Verschlüsselungsberichte erstellen und anzeigen

Sie können folgende Berichte erstellen:

- Bericht über den Verschlüsselungsstatus verwalteter Geräte. Dieser Bericht enthält Details zur Datenverschlüsselung verschiedener verwalteter Geräte. Der Bericht zeigt beispielsweise die Anzahl der Geräte, für welche die Richtlinie mit konfigurierten Verschlüsselungsregeln gilt. Außerdem können Sie ihm entnehmen, wie viele Geräte neu gestartet werden müssen. Darüber hinaus enthält der Bericht Informationen über die Verschlüsselungstechnologie und den Algorithmus für jedes Gerät.

- Bericht über den Verschlüsselungsstatus der Massenspeichergeräte. Dieser Bericht enthält ähnliche Informationen wie der Bericht zum Verschlüsselungsstatus verwalteter Geräte, verfügt aber lediglich über Informationen zu Massenspeichergeräten und Wechseldatenträgern.

- Bericht über Zugriffsrechte auf verschlüsselte Laufwerke. Dieser Bericht zeigt, welche Benutzerkonten Zugriff auf verschlüsselte Laufwerke haben.

- Bericht über Fehler bei der Dateiverschlüsselung. Dieser Bericht enthält Informationen über Fehler, die bei der Ausführung der Aufgaben zur Verschlüsselung und Entschlüsselung von Daten auf den Client-Geräten aufgetreten sind.

- Bericht über blockierte Zugriffe auf verschlüsselte Dateien. Dieser Bericht enthält Informationen über das Blockieren des Zugriffs von Anwendungen auf verschlüsselte Dateien. Dieser Bericht ist hilfreich, wenn nicht autorisierte Benutzer oder Anwendungen versuchen, auf verschlüsselte Dateien oder Laufwerke zuzugreifen.

Im Abschnitt **Überwachung und Berichterstattung** → **Berichte** können Sie jeden Bericht generieren. Alternativ können Sie im Abschnitt **Vorgänge** → **Verschlüsselung und Datenschutz** die folgenden Verschlüsselungsberichte generieren:

- Bericht über den Verschlüsselungsstatus der Massenspeichergeräte

- Bericht über Zugriffsrechte auf verschlüsselte Laufwerke

- Bericht über Fehler bei der Dateiverschlüsselung

*So generieren Sie einen Verschlüsselungsbericht im Abschnitt **Verschlüsselung und Datenschutz**:*

1. Stellen Sie sicher, dass Sie die Option **Verschlüsselung und Datenschutz anzeigen** in den Einstellungen der Benutzeroberfläche aktiviert haben.

2. Gehen Sie in den Eigenschaften für Richtlinien zur Registerkarte **Konfiguration von Ereignissen**.

3. Klicken Sie im Abschnitt **Kritisch** auf **Ereignis hinzufügen** und aktivieren Sie das Kontrollkästchen neben dem Ereignis *Fehler bei der Anwendung von Regeln zur Verschlüsselung / Entschlüsselung von Dateien*.

4. Klicken Sie auf die Schaltfläche **OK**.

5. Gehen Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz**.

6. Öffnen Sie einen der folgenden Abschnitte:

   - **Verschlüsselte Laufwerke**, erstellt den Bericht über den Verschlüsselungsstatus der Massenspeichergeräte oder den Bericht über Zugriffsrechte auf verschlüsselte Laufwerke.
   - **Verschlüsselungsereignisse** erstellt den Bericht über Fehler bei der Dateiverschlüsselung.

7. Klicken Sie auf den Namen des Berichts, den Sie erstellen möchten.

Die Erstellung des Berichts wird gestartet.

Zugriff auf ein verschlüsseltes Laufwerk im autonomen Modus gewähren

Ein Benutzer kann den Zugriff auf ein verschlüsseltes Gerät anfordern, wenn beispielsweise kein Kaspersky Endpoint Security für Windows auf dem verwalteten Gerät installiert ist. Nachdem Sie die Anforderung erhalten haben, können Sie eine Datei mit einem Zugriffsschlüssel erstellen und an den Benutzer senden. Alle Anwendungsfälle und detaillierten Anweisungen finden Sie in der Hilfe von Kaspersky Endpoint Security für Windows.

Um Zugriff auf ein sich im autonomen Modus befindliches, verschlüsseltes Laufwerk zu gewähren, gehen Sie wie folgt vor:

1. Rufen Sie eine Zugriffsanfrage-Datei von einem Benutzer ab (eine Datei mit der Erweiterung FDERTC). Folgen Sie den Anweisungen der Hilfe von Kaspersky Endpoint Security für Windows um die Datei in Kaspersky Endpoint Security für Windows zu generieren.
2. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Laufwerke**.

   Eine Liste mit den verschlüsselten Laufwerken wird geöffnet.
3. Wählen Sie das Laufwerk aus, für welches der Benutzer den Zugriff angefordert hat.
4. Klicken Sie auf die Schaltfläche **Zugriff auf das Gerät im autonomen Modus gewähren**.
5. Wählen Sie im folgenden Fenster das Plug-in aus, das der Kaspersky-Anwendung entspricht, mit dem das ausgewählte Laufwerk verschlüsselt wurde.

   Wenn ein Laufwerk mit einer Kaspersky-Anwendung verschlüsselt ist, das von Kaspersky Security Center Web Console nicht unterstützt wird, verwenden Sie die auf der Microsoft Management Console basierende Verwaltungskonsole, um den Offline-Zugriff zu gewähren.
6. Folgen Sie den Anweisungen in der Hilfe von Kaspersky Endpoint Security für Windows (siehe erweiterbare Blöcke am Ende des Abschnitts).

Anschließend kann der Benutzer die empfangene Datei verwenden, um auf das verschlüsselte Laufwerk zuzugreifen und die auf dem Laufwerk gespeicherten Daten zu lesen.

Benutzer und Benutzerrollen

In diesem Abschnitt werden Benutzer und Benutzerrollen beschrieben und Anweisungen zum Erstellen und Ändern dieser Regeln, zum Zuweisen von Rollen und Gruppen zu Benutzern sowie zum Zuordnen von Richtlinienprofilen zu Rollen zur Verfügung gestellt.

Über Benutzerrollen

Eine *Benutzerrolle* (auch als *Rolle* bezeichnet) ist ein Objekt, das einen Satz von Rechten und Berechtigungen enthält. Eine Rolle kann mit Einstellungen von Anwendungen von Kaspersky verbunden sein, die auf einem Benutzergerät installiert sind. Sie können einem Satz von Benutzern oder einem Satz von Sicherheitsgruppen eine Rolle auf jeder Hierarchieebene von Administrationsgruppen, Administrationsservern oder auf Ebene spezieller Objekte zuweisen.

Wenn Sie Geräte über eine Hierarchie von Administrationsservern verwalten, die auch virtuelle Administrationsserver umfasst, beachten Sie, dass Sie Benutzerrollen nur auf dem primären Administrationsserver erstellen, ändern oder löschen können. Anschließend können Sie die Benutzerrollen an sekundäre Administrationsserver weitergeben, einschließlich virtueller.

Sie können Benutzerrollen mit Richtlinienprofilen verbinden. Wenn einem Benutzer eine Rolle zugewiesen ist, erhält dieser Benutzer Sicherheitseinstellungen, die zur Durchführung der Aufgabenfunktionen erforderlich sind.

Eine Benutzerrolle kann mit Benutzern von Geräten in einer bestimmten Administrationsgruppe verbunden sein.

Benutzerrollenbereich

Ein *Benutzerrollenbereich* ist eine Kombination von Benutzern und Administrationsgruppen. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

Vorteil der Verwendung von Rollen

Ein Vorteil der Verwendung von Rollen ist, dass Sie Sicherheitseinstellungen nicht für jedes der verwalteten Geräte oder für jeden der Benutzer separat festlegen müssen. Die Anzahl von Benutzern und Geräten in einem Unternehmen kann recht groß sein, die Anzahl von unterschiedlichen Stellenfunktionen, für die unterschiedliche Sicherheitseinstellungen erforderlich sind, ist jedoch erheblich kleiner.

Unterschiede verglichen mit Verwendung von Richtlinienprofilen

Richtlinienprofile sind Eigenschaften einer Richtlinie, die für jede Kaspersky-Anwendung separat erstellt wird. Eine Rolle ist mit vielen Richtlinienprofilen verbunden, die für unterschiedliche Anwendungen erstellt wurden. Eine Rolle ist daher eine Methode zur Vereinigung von Einstellungen für einen bestimmten Benutzertyp an einem Ort.

Benutzerkonten und Sitzungen anzeigen

In Kaspersky Security Center können Benutzerkonten und Gruppen von Benutzerkonten verwaltet werden. Das Programm unterstützt zwei Typen von Benutzerkonten:

- Benutzerkonten der Mitarbeiter einer Organisation. Der Administrationsserver erhält Daten über die Benutzerkonten dieser Benutzer beim Abfragen des Unternehmensnetzwerks.
- Benutzerkonten für interne Benutzer. Diese werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Benutzerkonten für interne Benutzer werden nur innerhalb von Kaspersky Security Center erstellt und verwendet.

Sie können die Liste der Benutzerkonten und Sitzungen auf eine der folgenden Arten anzeigen:

- Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
- Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte** → Link <Gerätename> → Registerkarte **Allgemein** → Abschnitt **Allgemein** → Block **Sitzungen**.

  Im Abschnitt **Sitzungen** werden Benutzerkonten mit aktiven Sitzungen auf Windows-Geräten angezeigt.

Die Liste der Benutzerkonten und Sitzungen wird korrekt angezeigt, wenn die folgenden Voraussetzungen erfüllt sind:

- Sie verwenden den Administrationsagenten in der gleichen Version (oder höher) wie den Administrationsserver.
- Die Active Directory-Abfrage ist aktiviert, um die Benutzerkonten der Domänenbenutzer anzuzeigen.
- Auf verwalteten Windows-Geräten wird der Dienst **Server** (**LanmanServer**) ausgeführt.

Zugriffsrechte auf Programmfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle

Kaspersky Security Center bietet Unterstützungen für eine rollenbasierte Zugriffskontrolle auf die Funktionen von Kaspersky Security Center und von verwalteten Kaspersky-Anwendungen an.

Sie können die Zugriffsrechte auf Programmfunktionen für Benutzer von Kaspersky Security Center mit einer der folgenden Methoden konfigurieren:

- Durch individuelle Konfiguration der Berechtigungen jedes Benutzers bzw. jeder Benutzergruppe.
- Durch Erstellen typischer Benutzerrollen mit einer vordefinierten Auswahl von Berechtigungen und Zuweisung der Rollen an die Benutzer, wobei deren Verantwortungsbereiche berücksichtigt werden.

Die Verwendung von Benutzerrollen soll wiederkehrende Abläufe für das Konfigurieren von Zugriffsrechten der Benutzer auf Anwendungsfunktionen vereinfachen und verkürzen. Die Zugriffsberechtigungen werden in einer Rolle nach den typischen Aufgaben und Verantwortungsbereichen des Benutzers festgelegt.

Die Benutzerrollen können nach dem jeweiligen Verwendungszweck benannt werden. Sie können eine unbegrenzte Anzahl von Rollen in der Anwendung erstellen.

Sie können entweder vordefinierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen und die notwendigen Berechtigungen selbst konfigurieren.

Zugriffsrechte auf Programmfunktionen

Die untenstehende Tabelle gibt die Funktionen von Kaspersky Security Center mit den Zugriffsrechten für die Verwaltung der damit verknüpften Aufgaben, Berichte und Einstellungen, sowie für das Durchführen der damit verknüpften Benutzervorgänge an.

Um einen in der Tabelle aufgeführten Vorgang auszuführen, muss ein Benutzer die rechts neben dem Vorgang angegebene Berechtigung besitzen.

Die Berechtigungen **Lesen**, **Schreiben** und **Ausführen** können auf jede Aufgabe, jeden Bericht und jede Einstellung angewendet werden. Zusätzlich zu diesen Berechtigungen muss ein Benutzer über die Berechtigung **Vorgänge für die Geräteauswahlen ausführen** verfügen, um Aufgaben, Berichte oder Einstellungen auf Geräteauswahlen zu verwalten.

> Alle Aufgaben, Berichte, Einstellungen und Installationspakete, die in der Tabelle fehlen, gehören zum Funktionsbereich **Allgemeine Funktionen: Basisfunktionen**.

Zugriffsrechte auf Programmfunktionen

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: **Verwaltung von Administrationsgruppen**	**Schreiben**	• Hinzufügen eines Geräts zu einer Administrationsgruppe: **Schreiben** • Löschen eines Geräts aus einer Administrationsgruppe: **Schreiben** • Hinzufügen einer Administrationsgruppe zu einer anderen Administrationsgruppe: **Schreiben** • Löschen einer Administrationsgruppe aus einer anderen Administrationsgruppe: **Schreiben**	Keine

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: **Auf Objekte unabhängig von ihren ACLs zugreifen**	**Lesen**	Lesen auf alle Objekte erhalten: **Lesen**	Keine
Allgemeine Funktionen: **Basisfunktionen**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Regeln für das Verschieben von Geräten (erstellen, ändern, löschen) für den virtuellen Server: **Schreiben**, **Vorgänge für die Geräteauswahlen ausführen** • Benutzerdefiniertes Zertifikat des Mobilfunkprotokolls (LWNGT) erhalten: **Lesen** • Benutzerdefiniertes Zertifikat des Mobilfunkprotokolls (LWNGT) festlegen: **Schreiben** • NLA-definierte Netzwerkliste erhalten: **Lesen** • NLA-definierte Netzwerkliste hinzufügen, ändern oder löschen: **Schreiben** • Liste der Zugriffskontrolle von Gruppen anzeigen: **Lesen** • Kaspersky-Ereignisprotokoll anzeigen: **Lesen** • Anzeigen des Wiederherstellungsschlüssels, um den Zugriff auf eine mit BitLocker-Laufwerkverschlüsselung verschlüsselte Festplatte wiederherzustellen: **Ausführen**	• "Download von in die Datenver des Administrations • "Berichte sende • "Installationspa verteilen" • "Remote-Install einer Anwendu sekundären Administrations

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: **Gelöschte Objekte**	• **Lesen** • **Schreiben**	• Gelöschte Objekte im Papierkorb anzeigen: **Lesen** • Objekte aus dem Papierkorb löschen: **Schreiben**	Nichts
Allgemeine Funktionen: **Verarbeitung von Ereignissen**	• **Ereignisse löschen** • **Ereignisbenachrichtigungseinstellungen bearbeiten** • **Ereignisprotokollierungseinstellungen bearbeiten** • **Schreiben**	• Einstellungen der Ereignisregistrierung ändern: **Ereignisprotokollierungseinstellungen bearbeiten** • Einstellungen der Ereignisbenachrichtigung ändern: **Ereignisbenachrichtigungseinstellungen bearbeiten** • Ereignisse löschen: **Ereignisse löschen**	Nichts
Allgemeine Funktionen: **Vorgänge mit dem Administrationsserver**	• **Lesen** • **Schreiben** • **Ausführen** • **Objekt-ACLs ändern** • **Vorgänge für die Geräteauswahlen ausführen**	• Ports des Administrationsservers für die Verbindung zum Administrationsagenten angeben: **Schreiben** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy angeben: **Schreiben** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy für mobile Geräte angeben: **Schreiben** • Ports des Webservers für die Verteilung von autonomen Paketen angeben: **Schreiben** • Ports des Webservers für die Verteilung von MDM-Profilen angeben: **Schreiben**	• "Backup der Da Administrations anlegen" • "Pflege von Datenbanken"

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
		• SSL-Ports des Administrationsservers für die Verbindung mittels Kaspersky Security Center Web Console angeben: **Schreiben** • Ports des Administrationsservers für die Verbindung mit mobilen Geräten angeben: **Schreiben** • Maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind, angeben: **Schreiben** • Maximale Anzahl von Ereignissen, die der Administrationsserver versenden kann, angeben: **Schreiben** • Zeitspanne, in welcher Ereignisse durch den Administrationsserver versendet werden können, angeben: **Schreiben**	
Allgemeine Funktionen: **Bereitstellen von Kaspersky-Anwendungen**	• **Patches von Kaspersky verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	Die Installation von Patches akzeptieren oder ablehnen: **Patches von Kaspersky verwalten**	Nichts
Allgemeine Funktionen: **Lizenzschlüsselverwaltung**	• **Schlüsseldatei exportieren** • **Schreiben**	• Schlüsseldatei exportieren: **Schlüsseldatei exportieren** • Einstellungen des Lizenzschlüssels des Administrationsservers ändern: **Schreiben**	Nichts
Allgemeine Funktionen: **Erzwungene Berichtsverwaltung**	• **Lesen** • **Schreiben**	• Berichte unabhängig von ihren ACLs erstellen: **Schreiben** • Berichte unabhängig von ihren ACLs exportieren: **Lesen**	Nichts
Allgemeine Funktionen: **Hierarchie der Administrationsserver**	**Hierarchie der Administrationsserver konfigurieren**	Sekundäre Administrationsserver registrieren, aktualisieren oder löschen: **Hierarchie der Administrationsserver konfigurieren**	Nichts
Allgemeine Funktionen: **Benutzerberechtigungen**	**Objekt-ACLs ändern**	• "Sicherheit"-Eigenschaften eines jeden Objekts ändern: **Objekt-ACLs ändern** • Benutzerrollen verwalten: **Objekt-ACLs ändern** • Interne Benutzer verwalten: **Objekt-ACLs ändern** • Sicherheitsgruppen verwalten: **Objekt-ACLs ändern** • Anmeldenamen verwalten: **Objekt-ACLs ändern**	Nichts
Allgemeine Funktionen: **Virtuelle Administrationsserver**	• **Virtuelle Administrationsserver verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Liste mit virtuellen Administrationsservern abrufen: **Lesen** • Informationen über den virtuellen Administrationsserver erhalten: **Lesen** • Virtuellen Administrationsserver erstellen, aktualisieren oder löschen: **Virtuelle Administrationsserver verwalten** • Virtuellen Administrationsserver in andere Gruppe verschieben: **Virtuelle Administrationsserver verwalten** • Rechte des virtuellen Administrationsservers angeben: **Virtuelle Administrationsserver verwalten**	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: **Verwaltung der Chiffrierschlüssel**	**Schreiben**	Importieren von Chiffrierschlüsseln: **Schreiben**	Nichts
Verwaltung mobiler Geräte: Allgemein	• **Neue Geräte verbinden** • **Nur informative Befehle an mobile Geräte senden** • **Befehle an mobile Geräte senden** • **Zertifikate verwalten** • **Lesen** • **Schreiben**	• Wiederherstellungsdaten des Schlüsselverwaltungsdienstes abrufen: **Lesen** • Benutzerzertifikate löschen: **Zertifikate verwalten** • Öffentlichen Teil eines Benutzerzertifikats abrufen: **Lesen** • Aktivierung der Public-Key-Infrastruktur prüfen: **Lesen** • Konto der Public-Key-Infrastruktur prüfen: **Lesen** • Vorlagen der Public-Key-Infrastruktur abrufen: **Lesen** • Vorlagen der Public-Key-Infrastruktur nach Zertifikat der "Extended Key Usage" abrufen: **Lesen** • Widerruf des Zertifikats der Public-Key-Infrastruktur prüfen: **Lesen** • Einstellungen für die Ausstellung von Benutzerzertifikaten aktualisieren: **Zertifikate verwalten** • Einstellungen für die Ausstellung von Benutzerzertifikaten abrufen: **Lesen** • Pakete nach Programmname und Version abrufen: **Lesen** • Benutzerzertifikate einstellen oder abbrechen: **Zertifikate verwalten** • Benutzerzertifikate erneuern: **Zertifikate verwalten** • Tags für Benutzerzertifikate einstellen: **Zertifikate verwalten** • Erzeugung von MDM-Installationspaketen ausführen / abbrechen: **Neue Geräte verbinden**	Nichts
Systemverwaltung: Konnektivität	• **RDP-Sitzungen starten** • **Mit vorhandenen RDP-Sitzungen verbinden** • **Tunnelung starten** • **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Sitzung für Desktopfreigabe erstellen: **RDP-Sitzungen starten** • RDP-Sitzungen erstellen: **Mit vorhandenen RDP-Sitzungen verbinden** • Tunnel erstellen: **Tunnelung starten** • Liste mit Content-Netzwerken speichern: **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern**	Nichts
Systemverwaltung: Hardware-Inventur	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Objekt der Hardware-Inventarisierung abrufen oder exportieren: **Lesen** • Objekt der Hardware-Inventarisierung hinzufügen, einstellen oder löschen: **Schreiben**	Nichts
Systemverwaltung: Network Access Control (NAC)	• **Lesen** • **Schreiben**	• CISCO-Einstellungen anzeigen: **Lesen** • CISCO-Einstellungen ändern: **Schreiben**	Nichts
Systemverwaltung: Bereitstellung des Betriebssystems	• **PXE-Server bereitstellen** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Bereitstellung von PXE-Servern: **PXE-Server bereitstellen** • Liste mit PXE-Servern anzeigen: **Lesen** • Installationsprozess auf PXE-Clients starten oder stoppen: **Ausführen** • Treiber für WinPE und andere Betriebssysteme verwalten: **Schreiben**	"Installationspaket a eines Referenzimag einem Betriebssyste erstellen"
Systemverwaltung: Schwachstellen- und Patch-Management	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Eigenschaften von Patches von Drittanbietern anzeigen: **Lesen** • Eigenschaften von Patches von Drittanbietern ändern: **Schreiben**	• "Windows-Upda synchronisieren • "Updates von W Update installie

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
			• "Schwachstelle schließen" • "Erforderliche U installieren und Schwachsteller schließen"
Systemverwaltung: Remote-Installation	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	• Anzeigen von Drittanbieter-Installationspaketen, die auf dem Schwachstellen- und Patch-Management basieren: **Lesen** • Ändern von Drittanbieter-Installationspaketen, die auf dem Schwachstellen- und Patch-Management basieren: **Schreiben**	Nichts
Systemverwaltung: Software-Inventur	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	Nichts	Nichts
Systemverwaltung: Skripte remote ausführen	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge für die Geräteauswahlen ausführen**	Der Benutzer kann die Aufgabeneigenschaften anzeigen: **Lesen** Der Benutzer kann ein Installationspaket erstellen, löschen oder ändern: **Schreiben** Der Benutzer kann eine Aufgabe starten: **Schreiben**. Auf Client-Geräten unter Linux werden Skripte mit Root-Rechten ausgeführt. Der Benutzer kann eine Aufgabe ausführen oder deren Ausführung planen: **Ausführen** Der Benutzer kann eine Aufgabe auf einer Auswahl von Geräten ausführen: **Vorgänge für die Geräteauswahlen ausführen**	"Remote-Ausführur Skripten"

Vorkonfigurierte Benutzerrollen

Benutzer von Kaspersky Security Center mit zugewiesenen Benutzerrollen bekommen Zugriffsrechte auf Programmfunktionen gewährt.

Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Sie können entweder vordefinierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen. Beim Erstellen einer neuen Rolle müssen Sie den Gültigkeitsbereich der Rolle festlegen und die Zugriffsberechtigungen auf die Funktionen von Kaspersky Security Center selbst zuweisen. Einige der in Kaspersky Security Center verfügbaren, vorkonfigurierten Rollen können entsprechenden beruflichen Positionen, wie bspw. **Auditor**, **Security Officer** oder **Supervisor** zugeordnet werden (Diese Rollen stehen in Kaspersky Security Center ab der Version 11 zur Verfügung). Die Zugriffsberechtigungen dieser Rollen wurden gemäß den Standardaufgaben und den Tätigkeitsbereichen der entsprechenden Positionen vorkonfiguriert. Die folgende Tabelle gibt an, wie Rollen mit spezifischen beruflichen Positionen verbunden werden können.

Beispiele von Rollen für spezifische berufliche Positionen

Rolle	Kommentar
Auditor	Erlaubt alle Anzeigevorgänge und die Ausführung aller erstellten Aufgaben auf ausgewählten Geräten, die mit dem Administrationsserver über den Administrationsagenten mit lokalen Administratorrechten (root für Linux) verbunden sind. Es wird empfohlen, diese Rolle umsichtig zu gewähren und nur einer begrenzten Anzahl von Benutzern zuzuweisen, die diese Rechte zur Erfüllung ihrer offiziellen Verpflichtungen benötigen.
Supervisor	Erlaubt alle Anzeige-Vorgänge, erlaubt keine anderen Vorgänge. Sie können diese Rolle einem Security Officer und anderen Verantwortlichen zuweisen, die für die IT-Sicherheit in Ihrer Organisation zuständig sind.
Security Officer	Erlaubt alle Anzeige-Vorgänge, erlaubt Berichtsverwaltung; gewährt eingeschränkte Beschränkungen im Bereich **Systemverwaltung**: **Konnektivität**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.

Die folgende Tabelle gibt die jeder vorkonfigurierten Benutzerrolle zugewiesenen Zugriffsberechtigungen an.

Zugriffsberechtigungen von vorkonfigurierten Benutzerrollen

Rolle	Beschreibung
Administrator des Administrationsserver	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verarbeitung von Ereignissen** • **Hierarchie des Administrationsservers** • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Konnektivität** • **Hardware-Inventarisierung** • **Software-Inventur** Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.
Operator des Administrationsserver	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Konnektivität** • **Hardware-Inventarisierung** • **Software-Inventur**
Auditor	Gewährt alle Vorgänge in den Funktionsbereichen in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Gelöschte Objekte** • **Erzwungene Berichtsverwaltung** Sie können diese Rolle einer Person zuweisen, die das Audit Ihres Unternehmens durchführt.

Rolle	Beschreibung
Installationsadministrator	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Kaspersky software deployment** • **Verwaltung von Lizenzschlüsseln** • **Systemverwaltung**: • **Bereitstellung des Betriebssystems** • **Schwachstellen- und Patch-Management** • **Remote-Installation** • **Software-Inventur** Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen: Virtuelle Administrationsserver**.
Installationsoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verteilung der Software von Kaspersky** (gewährt auch die Funktion **Verwaltung der Patches von Kaspersky** in diesem Bereich) • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Bereitstellung des Betriebssystems** • **Schwachstellen- und Patch-Management** • **Remote-Installation** • **Software-Inventur**
Administrator von Kaspersky Endpoint Security	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.
Operator von Kaspersky Endpoint Security	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security
Hauptadministrator	Gewährt alle Vorgänge in Funktionsbereichen, *außer* für die folgenden Bereiche in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung** Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.

Rolle	Beschreibung
Hauptoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Gelöschte Objekte** • **Vorgänge auf dem Administrationsserver** • **Bereitstellen von Kaspersky-Anwendungen** • **Virtuelle Administrationsserver** • **Verwaltung mobiler Geräte: Allgemein** • **Systemverwaltung**, inklusive aller Funktionen • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security
Administrator der Funktion "Verwaltung mobiler Geräte"	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • **Verwaltung mobiler Geräte: Allgemein**
Operator der Funktion "Verwaltung mobiler Geräte"	Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen**: **Grundlegende Funktionen**. Gewährt die Berechtigungen **Lesen** und **Nur Informationsbefehle an mobile Geräte senden** in den Funktionsbereichen **Verwaltung mobiler Geräte**: **Allgemein**.
Security Officer	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung** Gewährt die Berechtigungen **Lesen**, **Schreiben**, **Ausführen**, **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** und **Ausführen von Vorgängen für die Geräteauswahlen** im Funktionsbereich **Systemverwaltung: Verbindungen**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.
Benutzer des Self Service Portals	Erlaubt alle Vorgänge im Funktionsbereich **Verwaltung mobiler Geräte: Self Service Portal**. Diese Funktionen wird nur von Kaspersky Security Center 11 oder höher unterstützt.
Supervisor	Gewährt die Berechtigung **Lesen** in den Funktionsbereichen **Allgemeine Funktionen**: **Zugriff auf Objekte, unabhängig von ihren ACLs** und **Allgemeine Funktionen**: **Erzwungene Berichtsverwaltung**. Sie können diese Rolle einem Security Officer und anderen Verantwortlichen zuweisen, die für die IT-Sicherheit in Ihrer Organisation zuständig sind.
Administrator der Funktionen "Schwachstellen- und Patch-Management"	Erlaubt alle Vorgänge in den Funktionsbereichen **Allgemeine Funktionen**: **Grundlegende Funktionen** und **Systemverwaltung** (einschließlich aller Funktionen).
Operator der Funktionen "Schwachstellen- und Patch-Management"	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in den Funktionsbereichen **Allgemeine Funktionen**: **Grundlegende Funktionen** und **Systemverwaltung** (einschließlich aller Funktionen).

Bestimmten Objekten Zugriffsrechte zuweisen

Neben der Zuweisung von Zugriffsrechten auf Ebene von Funktionsbereichen können Sie auch den Zugriff auf bestimmte Objekte konfigurieren, beispielsweise einer bestimmten Administrationsgruppe oder Aufgabe. Mit der Anwendung können Sie Zugriffsrechte für die folgenden Objekttypen festlegen:

- Administrationsgruppen
- Aufgaben
- Berichte

- Geräteauswahlen
- Ereignisauswahlen

So weisen Sie einem bestimmten Objekt Zugriffsrechte zu:

1. Gehen Sie je nach Objekttyp im Hauptmenü zum entsprechenden Abschnitt:
   - **Assets (Geräte) → Gruppenhierarchie**
   - **Assets (Geräte) → Aufgaben**
   - **Überwachung und Berichterstattung → Berichte**
   - **Assets (Geräte) → Geräteauswahlen**
   - **Überwachung und Berichterstattung → Ereignisauswahlen**
2. Öffnen Sie die Eigenschaften des Objekts, für das Sie Zugriffsrechte konfigurieren möchten.

   Um das Eigenschaftsfenster einer Administrationsgruppe oder einer Aufgabe zu öffnen, klicken Sie auf den Objektnamen. Eigenschaften anderer Objekte können über die Schaltfläche in der Werkzeugleiste geöffnet werden.
3. Gehen Sie im Eigenschaftenfenster zum Abschnitt **Zugriffsrechte**.

   Die Benutzerliste wird geöffnet. Die aufgelisteten Benutzer und Sicherheitsgruppen haben Zugriffsrechte auf das Objekt. Wenn Sie eine Hierarchie von Administrationsgruppen oder Servern verwenden, werden die Liste und die Zugriffsrechte standardmäßig von der übergeordneten Administrationsgruppe oder dem primären Server übernommen.
4. Um die Liste ändern zu können, aktivieren Sie die Option **Benutzerdefinierte Berechtigungen verwenden**.
5. Konfigurieren der Zugriffsrechte:
   - Verwenden Sie die Schaltflächen **Hinzufügen** und **Löschen**, um die Liste zu ändern.
   - Geben Sie für einen Benutzer oder eine Sicherheitsgruppe die Zugriffsrechte an. Führen Sie eine der folgenden Aktionen aus:
     - Wenn Sie Zugriffsrechte manuell festlegen möchten, wählen Sie den Benutzer oder die Sicherheitsgruppe aus, klicken Sie auf die Schaltfläche **Zugriffsrechte** und legen Sie anschließend die Zugriffsrechte fest.
     - Wenn Sie einem Benutzer oder einer Sicherheitsgruppe eine Benutzerrolle zuweisen möchten, wählen Sie den Benutzer oder die Sicherheitsgruppe aus, klicken Sie auf die Schaltfläche **Rollen** und wählen Sie anschließend die zuzuweisende Rolle aus.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Zugriffsrechte auf das Objekt sind konfiguriert.

Zuweisung von Zugriffsrechten an Benutzer und Sicherheitsgruppen

Sie können Benutzern und Sicherheitsgruppen Zugriffsrechte für die Nutzung verschiedener Funktionen des Administrationsservers zuweisen, z. B. für Kaspersky Endpoint Security für Linux.

So weisen Sie einem Benutzer oder einer Sicherheitsgruppe Zugriffsrechte zu:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Zugriffsrechte** das Kontrollkästchen neben dem Namen des Benutzers oder der Sicherheitsgruppe, dem bzw. der Rechte zugewiesen werden sollen, und klicken Sie dann auf die Schaltfläche **Zugriffsrechte**.

   Sie können nur einzelne Benutzer oder Sicherheitsgruppen auswählen. Wenn Sie mehr als ein Element auswählen, wird die Schaltfläche **Zugriffsrechte** deaktiviert.

3. Konfigurieren Sie die erforderlichen Rechte für den Benutzer oder die Gruppe:

   a. Erweitern Sie den Knoten mit den Funktionen des Administrationsservers oder einer anderen Kaspersky-Anwendung.

   b. Aktivieren Sie neben der gewünschten Funktion oder dem gewünschten Zugriffsrecht das Kontrollkästchen **Zulassen** oder **Verbieten**.

      Beispiel 1: Aktivieren Sie das Kontrollkästchen **Erlauben** neben dem Knoten **Anwendungsintegration**, um einem Benutzer oder einer Gruppe alle verfügbaren Zugriffsrechte für die Funktionen der Anwendungsintegration (**Lesen**, **Schreiben** und **Ausführen**) zu gewähren.

      Beispiel 2: Erweitern Sie den Knoten **Verwaltung von Chiffrierschlüsseln** und aktivieren Sie das Kontrollkästchen **Erlauben** neben **Schreibzugriff**, um einem Benutzer oder einer Gruppe das Zugriffsrecht **Schreiben** für die Funktion zur Verwaltung von Chiffrierschlüsseln zu gewähren.

4. Klicken Sie nach der Konfiguration der Zugriffsrechte auf **OK**.

Die Auswahl der Rechte für den Benutzer oder die Benutzergruppe wird angepasst.

Die Berechtigungen des Administrationsservers (oder der Administrationsgruppe) sind in die folgenden Bereiche unterteilt:

- Allgemeine Funktionen:
  - Verwaltung von Administrationsgruppen
  - Auf Objekte unabhängig von ihren ACLs zugreifen
  - Basisfunktionen
  - Gelöschte Objekte
  - Verwaltung der Chiffrierschlüssel
  - Verarbeitung von Ereignissen
  - Vorgänge mit dem Administrationsserver (nur im Eigenschaftsfenster des Administrationsservers)
  - Tags des Geräts
  - Bereitstellen von Kaspersky-Anwendungen
  - Lizenzschlüsselverwaltung

    - Programmintegration
    - Erzwungene Berichtsverwaltung
    - Hierarchie der Administrationsserver
    - Benutzerberechtigungen
    - Virtuelle Administrationsserver
- Verwaltung mobiler Geräte:
    - Allgemein
    - Self Service Portal
- Systemverwaltung:
    - Konnektivität
    - Skripte remote ausführen
    - Hardware-Inventur
    - Network Access Control (NAC)
    - Bereitstellung des Betriebssystems
    - Schwachstellen- und Patch-Management
    - Remote-Installation
    - Software-Inventur

Wenn für ein Zugriffsrecht weder **Zulassen** noch **Verbieten** ausgewählt ist, gilt das Zugriffsrecht als *Nicht festgelegt*: Der Zugriff wird verweigert, bis er für den Benutzer ausdrücklich verweigert oder erlaubt wird.

Die Rechte eines Benutzers setzen sich aus folgenden Faktoren zusammen:

- Eigene Rechte des Benutzers
- Rechte aller Rollen, die diesem Benutzer zugewiesen sind
- Rechte aller Sicherheitsgruppen, zu denen der Benutzer gehört
- Rechte aller Rollen, die den Sicherheitsgruppen zugewiesen sind, zu denen der Benutzer gehört

Wenn zumindest einer dieser Faktoren für eine Berechtigung den Status **Verbieten** hat, wird dem Benutzer diese Berechtigung verweigert, selbst wenn sie für andere Faktoren erlaubt oder nicht festgestellt ist.

Sie können auch Benutzer und Sicherheitsgruppen zum Umfang einer Benutzerrolle hinzufügen, um verschiedene Funktionen des Administrationsservers zu nutzen. Einstellungen, die einer Benutzerrolle zugeordnet sind, gelten nur für jene Geräte, die den Benutzern gehören, die diese Rolle innehaben, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verknüpft sind, einschließlich Untergruppen.

Benutzerkonto für einen internen Benutzer hinzufügen

Wenn Sie ein Benutzerkonto hinzufügen möchten, stellen Sie sicher, dass Ihr Konto die Berechtigung Objekt-ACLs ändern in dem Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" besitzt.

So fügen Sie ein neues internes Benutzerkonto zum Kaspersky Security Center hinzu:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im folgenden Fenster **Benutzer hinzufügen** die Einstellungen des neuen Benutzerkontos an:
   - **Name**
   - **Kennwort**

     Das Kennwort muss den folgenden Regeln entsprechen:
     - Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
     - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
       - Großbuchstaben (A–Z)
       - Kleinbuchstaben (a–z)
       - Ziffern (0–9)
       - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

     Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .

     Sie können die Option **Der Benutzer muss bei der ersten Anmeldung das Kennwort ändern** aktivieren, um bei der ersten Authentifizierung eines Benutzers eine Änderung des Kennworts zu erzwingen.
4. Speichern Sie die Änderungen, um die Erstellung des neuen Benutzerkontos abzuschließen.

Ein neues Benutzerkonto wird zur Liste mit Benutzern hinzugefügt.

Um sich mit einem erstellten internen Benutzerkonto an der Kaspersky Security Center Web Console anzumelden, müssen Sie diesem Konto eine Rolle zuweisen. Stellen Sie vor der Anmeldung sicher, dass dem internen Benutzerkonto eine Rolle zugewiesen wurde. Andernfalls tritt ein Anmeldefehler auf.

Eine Sicherheitsgruppe erstellen

Um eine Sicherheitsgruppen zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Gruppen** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Nehmen Sie im folgenden Fenster **Sicherheitsgruppe erstellen** die folgenden Einstellungen für die neue Sicherheitsgruppe vor:
   - **Gruppenname**
   - **Beschreibung**
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Eine neue Sicherheitsgruppe wird zur Liste mit Gruppen hinzugefügt.

Benutzerkonto eines internen Benutzers bearbeiten

Wenn Sie ein Benutzerkonto bearbeiten möchten, stellen Sie sicher, dass Ihr Konto die Berechtigung Objekt-ACLs ändern in dem Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" besitzt.

So bearbeiten Sie ein internes Benutzerkonto in Kaspersky Security Center:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf den Namen des Benutzerkontos, das Sie bearbeiten möchten.
3. Ändern Sie im folgenden Fenster für Benutzereinstellungen auf der Registerkarte **Allgemein** die Einstellungen für das Benutzerkonto:
   - **Benutzerstatus**

     Schalten Sie ggf. die Umschalttaste auf **Deaktiviert**, um zu verhindern, dass der Benutzer eine Verbindung zur Anwendung herstellt. Sie können ein Konto beispielsweise deaktivieren, nachdem ein Mitarbeiter das Unternehmen verlassen hat.
   - **Name**
   - **Vollständiger Name**
   - **Beschreibung**
   - **E-Mail-Adresse**
   - **Hauptrufnummer**

- **Kennwort**

  Bei Bedarf können Sie für die Verbindung des Benutzers zu Kaspersky Security Center ein neues Kennwort wie folgt festlegen:

  a. Klicken Sie auf die Schaltfläche **Kennwort ändern** und legen Sie anschließend ein neues Kennwort für das Benutzerkonto fest.

  Das Kennwort muss den folgenden Regeln entsprechen:

  - Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
  - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
    - Großbuchstaben (A–Z)
    - Kleinbuchstaben (a–z)
    - Ziffern (0–9)
    - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

  Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .

  b. Bei Bedarf können Sie die Option **Der Benutzer muss bei der ersten Anmeldung das Kennwort ändern** aktivieren, um bei der nächsten Authentifizierung eines Benutzers eine Änderung des Kennworts zu erzwingen.

  c. Wenn das Benutzerkonto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie über die Berechtigungen zur Kontoänderung verfügen. Geben Sie im Fenster **Schutz des Benutzerkontos** die Anmeldeinformationen des Benutzerkontos an, das über die Berechtigung Objekt-ACL ändern im Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" verfügt.

4. Auf der Registerkarte **Sicherheit für die Authentifizierung** können Sie die Sicherheitseinstellungen für dieses Benutzerkonto festlegen.

5. Auf der Registerkarte **Gruppen** können Sie einen Benutzer zu Sicherheitsgruppen hinzufügen.

6. Auf der Registerkarte **Geräte** können Sie einem Benutzer Geräte zuweisen.

7. Auf der Registerkarte **Rollen** können Sie einem Benutzer Rollen zuordnen.

8. Speichern Sie die Änderungen, um die Bearbeitung des Benutzerkontos abzuschließen.

Das aktualisierte Benutzerkonto wird in der Liste der Benutzer angezeigt.

Eine Sicherheitsgruppe bearbeiten

So bearbeiten Sie eine Sicherheitsgruppe:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Gruppen** aus.
2. Klicken Sie auf den Namen der Sicherheitsgruppe, die Sie bearbeiten möchten.
3. Ändern Sie im folgenden Fenster mit den Gruppeneinstellungen die Einstellungen für die Sicherheitsgruppe:
   - Auf der Registerkarte **Allgemein** können Sie die Einstellungen **Name** und **Beschreibung** ändern. Diese Einstellungen sind nur für interne Sicherheitsgruppen verfügbar.
   - Auf der Registerkarte **Benutzer** können Sie Benutzer zur Sicherheitsgruppe hinzufügen. Diese Einstellung ist nur für interne Benutzer und interne Sicherheitsgruppen verfügbar.
   - Auf der Registerkarte **Rollen** können Sie einer Sicherheitsgruppe eine Rolle zuweisen.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Änderungen werden auf die Sicherheitsgruppe angewendet.

Einem Benutzer oder einer Sicherheitsgruppe eine Rolle zuweisen

So weisen Sie einem Benutzer oder einer Sicherheitsgruppe eine Rolle zu:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** oder **Gruppen** aus.
2. Wählen Sie den Namen des Benutzers oder der Sicherheitsgruppe aus, dem oder der Sie die Rolle zuweisen wollen.

   Es können mehrere Namen ausgewählt werden.
3. Klicken Sie in der Menüleiste auf die Schaltfläche **Rolle zuordnen**.

   Der Assistent zum Zuweisen einer Rolle wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten: Wählen Sie die Rolle aus, die Sie den ausgewählten Benutzern oder Sicherheitsgruppen zuweisen wollen, und legen Sie anschließend den Gültigkeitsbereich der Rolle fest.

   Ein Benutzerrollenbereich ist eine Kombination von Benutzern und Administrationsgruppen. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

Als Ergebnis wird dem Benutzer, den Benutzern oder der Sicherheitsgruppe die Rolle mit einer Auswahl von Berechtigungen für die Arbeit mit dem Administrationsserver zugewiesen. In der Liste der Benutzer oder Sicherheitsgruppen wird in der Spalte **Zugeordnete Rollen** ein Kontrollkästchen angezeigt.

Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Benutzerkonten zu einer internen Sicherheitsgruppe hinzufügen

Einer internen Sicherheitsgruppe können nur die Benutzerkonten von internen Benutzern hinzugefügt werden.

So fügen Sie einer internen Sicherheitsgruppe Benutzerkonten hinzu:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Aktivieren Sie die Kontrollkästchen neben den Benutzerkonten, die Sie einer Sicherheitsgruppe hinzufügen möchten.
3. Klicken Sie auf die Schaltfläche **Gruppe zuordnen**.
4. Wählen Sie im folgenden Fenster **Gruppe zuordnen** die Sicherheitsgruppe aus, der Sie die Benutzerkonten hinzufügen möchten.
5. Klicken Sie auf **Speichern**.

Die Benutzerkonten werden der Sicherheitsgruppe hinzugefügt. Sie können interne Benutzer auch mithilfe der Gruppeneinstellungen zu einer Sicherheitsgruppe hinzufügen.

Benutzer zu Gerätebesitzern ernennen

Weitere Informationen darüber, wie man einen Benutzer zum Gerätebesitzer macht, entnehmen Sie der Hilfe von Kaspersky Secure Mobility Management.

So machen Sie einen Benutzer zum Gerätebesitzer:

1. Wenn Sie einem Gerät, das mit einem virtuellen Administrationsserver verbunden ist, einen Besitzer zuweisen möchten, wechseln Sie zunächst zum virtuellen Administrationsserver:
   a. Klicken Sie im Hauptmenü rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol ( ).
   b. Wählen Sie den gewünschten Administrationsserver aus.
2. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.

   Die Liste mit Benutzern wird geöffnet. Wenn Sie derzeit mit einem virtuellen Administrationsserver verbunden sind, enthält die Liste die Benutzer des aktuellen virtuellen Administrationsservers sowie des primären Administrationsservers.
3. Klicken Sie auf den Namen des Benutzerkontos, das Sie als Gerätebesitzer zuweisen möchten.
4. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Geräte**.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

6. Wählen Sie in der Geräteliste die Richtlinie aus, die Sie dem Benutzer zuweisen möchten.

7. Klicken Sie auf die Schaltfläche **OK**.

   Das ausgewählte Gerät wird zur Liste der dem Benutzer zugewiesenen Geräte hinzugefügt.

Derselbe Vorgang kann auch unter **Assets (Geräte)** → **Verwaltete Geräte** ausgeführt werden: Klicken Sie auf den Namen des Geräts, das Sie zuweisen möchten, und klicken Sie dann auf den Link **Gerätebesitzer verwalten**.

Konfigurieren der zweistufigen Überprüfung für alle Benutzer

In diesem Szenario wird beschrieben, wie Sie die zweistufige Überprüfung für alle Benutzer aktivieren und wie Benutzerkonten von der zweistufigen Überprüfung ausschließen. Wenn Sie die zweistufige Überprüfung für Ihr Benutzerkonto nicht aktiviert haben, bevor Sie es für andere Benutzer aktivieren, öffnet die Anwendung zunächst das Fenster zur Aktivierung der zweistufigen Überprüfung für Ihr Konto. In diesem Szenario wird außerdem beschrieben, wie Sie die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren.

> Wenn Sie die zweistufige Überprüfung für Ihr Benutzerkonto aktiviert haben, können Sie mit der Aktivierung der zweistufigen Überprüfung für alle Benutzer fortsetzen.

Erforderliche Vorrausetzungen

Vor dem Start:

- Stellen Sie sicher, dass Ihr Benutzerkonto über die Berechtigung zum Objekt-ACL ändern für den Funktionsbereich **Allgemeine Funktionen: Benutzerrechte** verfügt, um die Sicherheitseinstellungen für andere Benutzerkonten zu ändern.
- Stellen Sie sicher, dass die anderen Benutzer des Administrationsservers eine Authenticator-App auf ihren Geräten installieren.

Schritte

Das Aktivieren der zweistufigen Überprüfung für alle Benutzer erfolgt schrittweise:

1. **Installation einer Authenticator-App auf einem Gerät**

   Sie können jede Anwendung installieren, die den Algorithmus für zeitbasierte Einmalkennwörter (TOTP) unterstützt, z B:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA

Um zu überprüfen, ob Kaspersky Security Center die von Ihnen verwendete Authenticator-App unterstützt, aktivieren Sie die Zwei-Faktor-Authentifikation für alle Benutzer oder für einen bestimmten Benutzer.

Einer der Schritte schlägt vor, dass Sie den Sicherheitscode angeben, der von der Authenticator-App generiert wird. Wenn dies erfolgreich ist, unterstützt Kaspersky Security Center den ausgewählten Authenticator.

Wir raten dringend davon ab, die Authenticator-App auf demselben Gerät zu installieren, von dem aus die Verbindung zum Administrationsserver hergestellt wird.

2. **Synchronisation der Zeit der Authenticator-App mit der Zeit des Gerätes, auf dem der Administrationsserver installiert ist**

   Stellen Sie mithilfe externer Zeitquellen sicher, dass die Uhrzeit auf dem Gerät mit der Authenticator-App und die Uhrzeit auf dem Gerät mit dem Administrationsserver mit der UTC-Zeit synchronisiert sind. Andernfalls können Fehler bei der Authentifizierung und Aktivierung der zweistufigen Überprüfung auftreten.

3. **Aktivieren der zweistufigen Überprüfung für Ihr Benutzerkonto und Anfordern des geheimen Schlüssels für Ihr Benutzerkonto**

   Anleitung:

   - Für die Verwaltungskonsole auf MMC-Basis: die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren
   - Für die Kaspersky Security Center Web Console: die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren

   Nachdem Sie die zweistufige Überprüfung für Ihr Benutzerkonto aktiviert haben, können Sie die zweistufige Überprüfung für alle Benutzer aktivieren.

4. **Zweistufige Überprüfung für alle Benutzer aktivieren**

   Benutzer, für welche die zweistufige Überprüfung aktiviert ist, müssen diese verwenden, um sich am Administrationsserver anmelden.

   Anleitung:

   - Für die Verwaltungskonsole auf MMC-Basis: die zweistufige Überprüfung für alle Benutzer aktivieren
   - Für die Kaspersky Security Center Web Console: die zweistufige Überprüfung für alle Benutzer aktivieren

5. **Den Namen eines Sicherheitscode-Ausstellers bearbeiten**

   Wenn Sie mehrere Administrationsserver mit ähnlichen Namen haben, müssen Sie möglicherweise die Namen der Sicherheitscode-Aussteller ändern, um verschiedene Administrationsserver besser unterscheiden zu können.

   Anleitung:

   - Für die Verwaltungskonsole auf MMC-Basis: Namen des Sicherheitscode-Ausstellers bearbeiten
   - Für Kaspersky Security Center Web Console: Namen eines Sicherheitscode-Ausstellers bearbeiten

6. **Ausschließen der Benutzerkonten, für die Sie die zweistufige Überprüfung nicht aktivieren müssen**

   Bei Bedarf können Sie Benutzerkonten von der zweistufigen Überprüfung ausschließen. Benutzer mit ausgeschlossenen Benutzerkonten müssen sich nicht mittels zweistufiger Überprüfung am Administrationsserver anmelden.

Anleitung:

- Für die Verwaltungskonsole auf MMC-Basis: Benutzerkonten von der zweistufigen Überprüfung für ausschließen
- Für Kaspersky Security Center Web Console: Benutzerkonten von der zweistufigen Überprüfung ausschließen

7. **Zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren**

   Wenn die Benutzer nicht von der zweistufigen Überprüfung ausgeschlossen sind und die zweistufige Überprüfung für deren Benutzerkonten noch nicht konfiguriert ist, müssen sie diese in dem Fenster konfigurieren, das sich bei der Anmeldung an Kaspersky Security Center öffnet. Andernfalls können sie nicht entsprechend ihren Rechten auf den Administrationsserver zugreifen.

   Anleitung:

   - Für die Verwaltungskonsole auf MMC-Basis: Die zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren
   - Für die Kaspersky Security Center Web Console: Die zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren

Ergebnisse

Nach Abschluss dieses Szenarios:

- Die zweistufige Überprüfung ist für Ihr Konto aktiviert.
- Die zweistufige Überprüfung ist für alle Benutzerkonten des Administrationsservers aktiviert, mit Ausnahme der Benutzerkonten, die ausgeschlossenen wurden.

Über die zweistufige Überprüfung

Wenn die zweistufige Überprüfung für ein Benutzerkonto aktiviert ist, ist für die Anmeldung an der Verwaltungskonsole oder in Kaspersky Security Center Web Console neben dem Benutzernamen und dem Kennwort ein einmaliger Sicherheitscode erforderlich. Wenn die Domänenauthentifizierung aktiviert ist, muss der Benutzer nur den Einmal-Sicherheitscode eingeben.

Um die zweistufige Überprüfung zu verwenden, installieren Sie auf dem mobilen Gerät oder Computer eine Authenticator-App, die Einmal-Sicherheitscodes generieren kann. Sie können jedes Programm installieren, das den TOTP-Algorithmus (Time-based One-time Password) unterstützt, z B:

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA

Um zu überprüfen, ob Kaspersky Security Center die von Ihnen verwendete Authenticator-App unterstützt, aktivieren Sie die Zwei-Faktor-Authentifikation für alle Benutzer oder für einen bestimmten Benutzer.

Einer der Schritte schlägt vor, dass Sie den Sicherheitscode angeben, der von der Authenticator-App generiert wird. Wenn dies erfolgreich ist, unterstützt Kaspersky Security Center den ausgewählten Authenticator.

Es wird dringend empfohlen, dass Sie den geheimen Schlüssel oder QR-Code speichern und an einem sicheren Ort aufbewahren. Auf diese Weise können Sie den Zugriff auf die Kaspersky Security Center Web Console wiederherstellen, falls Sie den Zugriff auf Ihr mobiles Gerät verlieren.

Um die Verwendung von Kaspersky Security Center abzusichern, können Sie die zweistufige Überprüfung für Ihr eigenes Konto und die zweistufige Überprüfung für alle Benutzer aktivieren.

Sie können Benutzerkonten von der zweistufigen Überprüfung ausschließen. Dies kann für Dienstkonten erforderlich sein, die den zur Authentifizierung notwendigen Sicherheitscode nicht empfangen können.

Regeln und Einschränkungen

Um die zweistufige Überprüfung für alle Benutzer zu aktivieren und nur für bestimmte Benutzer zu deaktivieren:

- Stellen Sie sicher, dass Sie die Berechtigung Objekt-ACLs ändern in dem Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** besitzen.
- Aktivieren Sie die zweistufige Überprüfung für Ihr Konto.

So aktivieren Sie die zweistufige Überprüfung für alle Benutzer:

- Stellen Sie sicher, dass Sie die Berechtigung Objekt-ACLs ändern in dem Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** besitzen.
- Melden Sie sich an der Kaspersky Security Center Web Console mithilfe der zweistufigen Überprüfung an.

Wenn für ein Benutzerkonto auf dem Kaspersky Security Center Administrationsserver ab Version 13 eine zweistufige Überprüfung aktiviert ist, kann sich der Benutzer nicht an der Kaspersky Security Center Web Console in den Versionen 12, 12.1 oder 12.2 anmelden.

Erneutes Ausstellen des geheimen Schlüssels

Jeder Benutzer kann den geheimen Schlüssel, der für die zweistufige Überprüfung verwendet wird, neu ausstellen. Wenn sich ein Benutzer am Administrationsserver mit dem neu ausgestellten geheimen Schlüssel anmeldet, wird der neue geheime Schlüssel für das Benutzerkonto gespeichert. Wenn der Benutzer den neuen geheimen Schlüssel falsch eingibt, wird der neue geheime Schlüssel nicht gespeichert und der aktuelle geheime Schlüssel bleibt gültig.

Ein Sicherheitscode besitzt eine Kennung, die als *Aussteller-Name* bezeichnet wird. Der Name des Sicherheitscode-Ausstellers wird als Kennung des Administrationsservers in der Authenticator-App verwendet. Der Standardwert für den Namen des Sicherheitscode-Ausstellers entspricht dem Namen des Administrationsservers. Sie können den Namen des Sicherheitscode-Ausstellers ändern. Wenn Sie den Namen des Sicherheitscode-Ausstellers ändern, müssen Sie einen neuen geheimen Schlüssel ausstellen und an die Authenticator-App übergeben.

Die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren (Web Console)

Sie können die zweistufige Überprüfung nur für Ihr eigenes Konto aktivieren.

Stellen Sie sicher, dass auf dem mobilen Gerät eine Authenticator-App installiert ist, bevor Sie die zweistufige Überprüfung für Ihr Konto aktivieren. Stellen Sie sicher, dass die in der Authenticator-App festgelegte Zeit mit der Zeit auf dem Gerät, auf dem der Administrationsserver installiert ist, synchronisiert wird.

So aktivieren Sie die zweistufige Überprüfung für ein Benutzerkonto:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer**.
2. Klicken Sie auf den Namen Ihres Benutzerkontos.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Sicherheit für die Authentifizierung**.
4. Auf der Registerkarte **Sicherheit für die Authentifizierung**:
   a. Wählen Sie die Option **Benutzername, Kennwort und Sicherheitscode abfragen (zweistufige Überprüfung)** aus. Klicken Sie auf **Speichern**.
   b. Klicken Sie im folgenden Fenster der zweistufigen Überprüfung auf **So richten Sie die zweistufige Überprüfung ein**.
      Geben Sie den geheimen Schlüssel in die Authenticator-App ein oder klicken Sie auf **QR-Code anzeigen** und scannen Sie den QR-Code mit der Authenticator-App des mobilen Geräts, um einen einmaligen Sicherheitscode zu erhalten.
   c. Geben Sie im Fenster zur zweistufige Überprüfung den Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie dann auf **Überprüfen und anwenden**.
5. Klicken Sie auf **Speichern**.

Die zweistufige Überprüfung ist für Ihr Konto aktiviert.

Zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren (MMC-basiert)

Stellen Sie sicher, dass auf dem mobilen Gerät eine Authenticator-App installiert ist, bevor Sie die zweistufige Überprüfung für Ihr Konto aktivieren. Stellen Sie sicher, dass die in der Authenticator-App festgelegte Zeit mit der Zeit des Administrationsservers synchronisiert wird.

So aktivieren Sie die zweistufige Überprüfung für Ihr Konto:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.

2. Wechseln Sie im Eigenschaftenfenster des Administrationsservers zum Bereich **Abschnitte** und wählen Sie **Erweitert** und anschließend **Zweistufige Überprüfung** aus.

3. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf **Einrichten**.

   > Wenn die zweistufige Überprüfung für Ihr Konto bereits aktiviert ist, können Sie durch Klicken der Schaltfläche **Einrichten** den geheimen Schlüssel zurücksetzen und die zweistufige Überprüfung erneut konfigurieren.

   Im folgenden Fenster mit Eigenschaften der zweistufigen Überprüfung wird der geheime Schlüssel angezeigt.

4. Geben Sie den geheimen Schlüssel in die Authenticator-App ein, um einen Einmal-Sicherheitscode zu erhalten. Sie können den geheimen Schlüssel manuell in der Authenticator-App eingeben oder den QR-Code mit der Authenticator-App auf dem mobilen Gerät scannen.

5. Geben Sie den von der Authenticator-App generierten Sicherheitscode an und klicken Sie anschließend auf die Schaltfläche **OK**, um das Fenster mit den Eigenschaften der zweistufigen Überprüfung zu schließen.

6. Klicken Sie auf die Schaltfläche **Anwenden**.

7. Klicken Sie auf die Schaltfläche **OK**.

Die zweistufige Überprüfung ist für Ihr eigenes Konto aktiviert.

Obligatorische zweistufige Überprüfung für alle Benutzer aktivieren (Web Console)

Sie können die zweistufige Überprüfung für alle Benutzer des Administrationsservers aktivieren, wenn Ihr Benutzerkonto über die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und wenn Sie sich mittels zweistufiger Überprüfung authentifiziert haben.

So aktivieren Sie die zweistufige Überprüfung für alle Benutzer:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Schalten Sie in der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters den Umschalter für die **zweistufige Überprüfung für alle Benutzer** in die Position "aktiviert".

3. Wenn Sie keine zweistufige Überprüfung für Ihr Benutzerkonto aktiviert haben, öffnet die Anwendung das Fenster zum Aktivieren der zweistufigen Überprüfung für Ihr eigenes Konto.

   a. Klicken Sie im Fenster der zweistufigen Überprüfung auf **So richten Sie die zweistufige Überprüfung ein**.

   b. Geben Sie den geheimen Schlüssel manuell in die Authenticator-App ein oder klicken Sie auf **QR-Code anzeigen** und scannen Sie den QR-Code mit der Authenticator-App Ihres des Geräts, um einen einmaligen Sicherheitscode zu erhalten.

   c. Geben Sie im Fenster zur zweistufigen Überprüfung den Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie anschließend auf **Überprüfen und anwenden**.

Die zweistufige Überprüfung wurde für alle Benutzer aktiviert. Von nun an müssen Benutzer des Administrationsservers, einschließlich der Benutzer, die nach der Aktivierung der zweistufigen Überprüfung hinzugefügt wurden, die zweistufige Überprüfung für ihre Konten konfigurieren. Ausgenommen sind Benutzer, die von der zweistufigen Überprüfung ausgeschlossen sind.

Zweistufige Überprüfung für alle Benutzer aktivieren (MMC-basiert)

Sie können die zweistufige Überprüfung für alle Benutzer des Administrationsservers aktivieren, wenn Ihr Benutzerkonto über die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und wenn Sie sich mittels zweistufiger Überprüfung authentifiziert haben.

So aktivieren Sie die zweistufige Überprüfung für alle Benutzer:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.

2. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Bereich **Abschnitte** zuerst **Erweitert** und anschließend **Zweistufige Überprüfung** aus.

3. Klicken Sie auf die Schaltfläche **Als zwingend festlegen**, um die zweistufige Überprüfung für alle Benutzer zu aktiveren.

4. Wenn Sie die zweistufige Überprüfung für Ihr Benutzerkonto nicht aktiviert haben, öffnet die Anwendung das Fenster zum Aktivieren der zweistufigen Überprüfung für Ihr eigenes Konto.

   a. Geben Sie den geheimen Schlüssel in die Authenticator-App ein, um einen Einmal-Sicherheitscode zu erhalten. Sie können den geheimen Schlüssel manuell in der Authenticator-App eingeben oder den QR-Code mit der Authenticator-App auf dem mobilen Gerät scannen, um einen Einmal-Sicherheitscode zu erhalten.

   b. Geben Sie den von der Authenticator-App generierten Sicherheitscode an und klicken Sie anschließend auf die Schaltfläche **OK**, um das Fenster mit den Eigenschaften der zweistufigen Überprüfung zu schließen.

5. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf die Schaltfläche **Übernehmen** und klicken Sie **OK**.

Die zweistufige Überprüfung ist für alle Benutzer aktiviert. Von nun an müssen alle Benutzer des Administrationsservers, einschließlich der Benutzer, die nach Aktivierung dieser Option hinzugefügt wurden, die zweistufige Überprüfung für ihre Benutzerkonten konfigurieren. Ausgenommen sind Benutzer, deren Konten von der zweistufigen Überprüfung ausgeschlossen sind.

Zweistufige Überprüfung für ein Benutzerkonto deaktivieren (Web Console)

Sie können die zweistufige Überprüfung für Ihr eigenes Benutzerkonto sowie für das Konto eines anderen Benutzers deaktivieren.

Sie können die zweistufige Überprüfung das Konto eines anderen Benutzers deaktivieren, wenn Ihr Benutzerkonto über die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und wenn Sie sich mittels zweistufiger Überprüfung authentifiziert haben.

So deaktivieren Sie die zweistufige Überprüfung für ein Benutzerkonto:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer**.
2. Klicken Sie auf den Namen des internen Benutzerkontos, für das Sie die zweistufige Überprüfung deaktivieren möchten. Dies kann Ihr eigenes Benutzerkonto oder das Konto eines anderen Benutzers sein.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.
4. Wählen Sie auf der Registerkarte **Schutz des Benutzerkontos** die Option **Nur Benutzername und Kennwort abfragen**, wenn Sie die zweistufige Überprüfung für ein Benutzerkonto deaktivieren möchten.
5. Klicken Sie auf **Speichern**.

Die zweistufige Überprüfung ist jetzt für das Benutzerkonto deaktiviert.

Wenn sich ein Benutzer nicht mehr mit der zweistufigen Überprüfung an der Kaspersky Security Center Web Console anmelden kann und Sie seinen Zugriff wiederherstellen möchten, deaktivieren Sie die zweistufige Überprüfung für dieses Benutzerkonto und wählen Sie anschließend die Option **Nur Benutzername und Kennwort abfragen** wie oben beschrieben aus. Melden Sie sich anschließend in der Kaspersky Security Center Web Console mit dem Benutzerkonto an, für das Sie die zweistufige Überprüfung deaktiviert haben, und aktivieren Sie die Überprüfung erneut.

Zweistufige Überprüfung für ein Benutzerkonto deaktivieren (MMC-basiert)

So deaktivieren Sie die zweistufige Überprüfung für Ihr eigenes Konto:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.
2. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Bereich **Abschnitte** zuerst **Erweitert** und anschließend **Zweistufige Überprüfung** aus.
3. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf **Deaktivieren**.
4. Klicken Sie auf die Schaltfläche **Anwenden**.
5. Klicken Sie auf die Schaltfläche **OK**.

Die zweistufige Überprüfung ist für Ihr Konto deaktiviert.

Sie können die zweistufige Überprüfung von anderen Benutzerkonten deaktivieren. Dies bietet beispielsweise Schutz für den Fall, wenn ein Benutzer ein mobiles Gerät verliert oder es beschädigt wird.

Sie können die zweistufige Überprüfung für das Konto eines anderen Benutzers nur dann deaktivieren, wenn Ihr Benutzerkonto über die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und wenn Sie sich mittels zweistufiger Überprüfung authentifiziert haben. Durch das Ausführen der folgenden Schritte können Sie die zweistufige Überprüfung auch für Ihr eigenes Konto deaktivieren.

So deaktivieren Sie die zweistufige Überprüfung für jedes Benutzerkonto:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Benutzerkonten**.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.

2. Doppelklicken Sie im Arbeitsbereich auf das Benutzerkonto, für das Sie die zweistufige Überprüfung deaktivieren möchten.

   Für alle Benutzerkonten, für welche die zweistufige Überprüfung aktiviert wird, ist die Spalte **2FA erforderlich** auf **Ja** gesetzt.

3. Wählen Sie im folgenden Fenster **Eigenschaften: <Benutzername>** den Abschnitt **Zweistufige Überprüfung**.

4. Wählen Sie im Abschnitt **Zweistufige Überprüfung** die folgenden Optionen aus:

   - Wenn Sie die zweistufige Überprüfung für ein Benutzerkonto deaktivieren möchten, klicken Sie auf die Schaltfläche **Deaktivieren**.

   - Wenn Sie dieses Benutzerkonto von der zweistufigen Überprüfung ausschließen möchten, wählen Sie die Option **Der Benutzer kann sich nur unter Verwendung von Benutzername und Kennwort anmelden**.

5. Klicken Sie auf die Schaltfläche **Anwenden**.

6. Klicken Sie auf die Schaltfläche **OK**.

Die zweistufige Überprüfung für ein Benutzerkonto ist deaktiviert.

Wenn Sie den Zugriff für einen Benutzers, der sich nicht mithilfe der zweistufigen Überprüfung an der Verwaltungskonsole anmelden kann, wiederherstellen möchten, deaktivieren Sie die zweistufige Überprüfung für dieses Benutzerkonto und wählen Sie in der **Zweistufigen Überprüfung** die Option **Der Benutzer kann sich nur unter Verwendung von Benutzername und Kennwort anmelden** wie oben beschrieben. Melden Sie sich anschließend in der Verwaltungskonsole mit dem Benutzerkonto an, für das Sie die zweistufige Überprüfung deaktiviert haben, und aktivieren Sie die Überprüfung erneut.

Obligatorische zweistufige Überprüfung für alle Benutzer deaktivieren (Web Console)

Sie können die erforderliche zweistufige Überprüfung für alle Benutzer deaktivieren, wenn die zweistufige Überprüfung für Ihr Benutzerkonto aktiviert ist und Ihr Konto die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** hat. Wenn die zweistufige Überprüfung für Ihr Benutzerkonto nicht aktiviert ist, müssen Sie die zweistufige Überprüfung für Ihr Konto aktivieren, bevor Sie diese für alle Benutzer deaktivieren.

So deaktivieren Sie die zweistufige Überprüfung für alle Benutzer:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Setzen Sie in der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters den Umschalter für die **zweistufige Überprüfung für alle Benutzer** in die Position "Deaktiviert".

Die zweistufige Überprüfung wurde für alle Benutzer deaktiviert. Die Deaktivierung der zweistufigen Überprüfung für alle Benutzer erstreckt sich nicht auf bestimmte Konten, für welche die zweistufige Überprüfung zuvor separat aktiviert wurde.

Obligatorische zweistufige Überprüfung für alle Benutzer deaktivieren (MMC-basiert)

Sie können die erforderliche zweistufige Überprüfung für alle Benutzer des Administrationsservers deaktivieren, wenn Sie über die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügen und wenn Sie sich mittels zweistufiger Überprüfung authentifiziert haben.

So deaktivieren Sie die zweistufige Überprüfung für alle Benutzer:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.

2. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Bereich **Abschnitte** zuerst **Erweitert** und anschließend **Zweistufige Überprüfung** aus.

3. Klicken Sie auf die Schaltfläche **Als optional festlegen**, um die zweistufige Überprüfung für alle Benutzer zu deaktivieren.

4. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf **Annehmen**.

5. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf **OK**.

Die zweistufige Überprüfung wurde für alle Benutzer deaktiviert. Die Deaktivierung der zweistufigen Überprüfung für alle Benutzer erstreckt sich nicht auf bestimmte Konten, für welche die zweistufige Überprüfung zuvor separat aktiviert wurde.

Benutzerkonten von der zweistufigen Überprüfung ausschließen (Web Console)

Sie können Benutzerkonten von der zweistufigen Überprüfung ausschließen, wenn Sie die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** haben.

Wenn ein Benutzerkonto aus der Liste der zweistufigen Überprüfung für alle Benutzer ausgeschlossen ist, muss dieser Benutzer die zweistufige Überprüfung nicht verwenden.

Das Ausschließen von Benutzerkonten von der zweistufigen Überprüfung kann für Dienstkonten erforderlich sein, die den Sicherheitscode während der Authentifikation nicht übertragen können.

So schließen Sie bestimmte Benutzerkonten von der zweistufigen Überprüfung aus:

1. Müssen Sie eine Abfrage des Microsoft Active Directory-Domänencontrollers ausführen, um die Liste der Administrationsserver-Benutzer zu aktualisieren, wenn Sie Active Directory-Konten ausschließen möchten.
2. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
3. Klicken Sie auf der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters, in der Tabelle mit den Ausschlüssen aus der zweistufigen Überprüfung, auf die Schaltfläche **Hinzufügen**.
4. Führen Sie in dem neuen Fenster folgende Schritte aus:

   a. Wählen Sie die Benutzerkonten aus, die Sie ausschließen möchten.

   b. Klicken Sie auf **OK**.

Die ausgewählten Benutzerkonten werden von der zweistufigen Überprüfung ausgeschlossen.

Benutzerkonten von der zweistufigen Überprüfung ausschließen (MMC-basiert)

Sie können ein Benutzerkonto von der zweistufigen Überprüfung ausschließen, wenn Ihr Benutzerkonto die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** hat.

Wenn ein Benutzerkonto von der zweistufigen Überprüfung ausgeschlossen ist, kann sich dieser Benutzer ohne Verwendung der zweistufigen Überprüfung an der Verwaltungskonsole oder der Kaspersky Security Center Web Console anmelden.

> Das Ausschließen von Benutzerkonten von der zweistufigen Überprüfung kann für Dienstkonten erforderlich sein, die den Sicherheitscode während der Authentifikation nicht übergeben können.

Um ein Benutzerkonto von der zweistufigen Überprüfung auszuschließen:

1. Wenn Sie ein Active Directory-Konto ausschließen möchten, führen Sie eine Active Directory-Abfrage durch, um die Liste mit den Benutzern des Administrationsservers zu aktualisieren.
2. Öffnen Sie in der Konsolenstruktur den Ordner **Benutzerkonten**.

   Der Ordner **Benutzerkonten** ist standardmäßig ein Unterordner des Ordners **Erweitert**.
3. Doppelklicken Sie im Arbeitsbereich auf das Benutzerkonto, das Sie von der zweistufigen Überprüfung ausschließen möchten.
4. Wählen Sie im folgenden Fenster **Eigenschaften: <Benutzername>** den Abschnitt **Zweistufige Überprüfung**.
5. Wählen Sie im angezeigten Abschnitt die Option **Der Benutzer kann sich nur unter Verwendung von Benutzername und Kennwort anmelden**.
6. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf die Schaltfläche **Übernehmen** und klicken Sie **OK**.

Dieses Benutzerkonto wird von der zweistufigen Überprüfung ausgeschlossen. Sie können die ausgeschlossenen Konten in der Liste der Benutzerkonten überprüfen.

Den Namen eines Sicherheitscode-Ausstellers bearbeiten (Web Console)

Möglicherweise haben Sie mehrere Identifikatoren (auch "Aussteller" genannt) für verschiedene Administrationsserver. Sie können den Namen eines Sicherheitscode-Ausstellers ändern, beispielsweise wenn der Administrationsserver bereits einen ähnlichen Namen eines Sicherheitscode-Ausstellers für einen anderen Administrationsserver verwendet. Standardmäßig entspricht der Name eines Sicherheitscode-Ausstellers dem Namen des Administrationsservers.

Nachdem Sie den Namen des Sicherheitscode-Ausstellers geändert haben, müssen Sie einen neuen geheimen Schlüssel ausstellen und an die Authenticator-App übergeben.

So geben Sie einen neuen Namen des Sicherheitscode-Ausstellers an:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.

3. Klicken Sie auf der Registerkarte **Schutz des Benutzerkontos** auf den Link **Bearbeiten**.

   Der Abschnitt **Aussteller des Sicherheitscodes ändern** wird geöffnet.

4. Geben Sie einen neuen Namen für den Sicherheitscode-Aussteller an.

5. Klicken Sie auf **OK**.

Für den Administrationsserver wird ein neuer Name des Sicherheitscode-Ausstellers angezeigt.

Name eines Sicherheitscode-Ausstellers bearbeiten (MMC-basiert)

Möglicherweise haben Sie mehrere Identifikatoren (auch "Aussteller" genannt) für verschiedene Administrationsserver. Sie können den Namen eines Sicherheitscode-Ausstellers ändern, beispielsweise wenn der Administrationsserver bereits einen ähnlichen Namen eines Sicherheitscode-Ausstellers für einen anderen Administrationsserver verwendet. Standardmäßig entspricht der Name eines Sicherheitscode-Ausstellers dem Namen des Administrationsservers.

Nachdem Sie den Namen des Sicherheitscode-Ausstellers geändert haben, müssen Sie einen neuen geheimen Schlüssel ausstellen und an die Authenticator-App übergeben.

Um einen neuen Namen für einen Sicherheitscode-Aussteller anzugeben:

1. Öffnen Sie im Konsolenbaum von Kaspersky Security Center mit der rechten Maustaste das Kontextmenü des Knotens **Administrationsserver** und wählen Sie anschließend den Punkt **Eigenschaften** aus.

2. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Bereich **Abschnitte** zuerst **Erweitert** und anschließend **Zweistufige Überprüfung** aus.

3. Geben Sie im Feld **Sicherheitscode ausgestellt von** einen neuen Namen für den Aussteller des Sicherheitscodes an.

4. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf **Annehmen**.

5. Klicken Sie im Abschnitt **Zweistufige Überprüfung** auf **OK**.

Für den Administrationsserver wird jetzt ein neuer Name des Sicherheitscode-Ausstellers angezeigt.

Die zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren (Web Console)

Wenn Sie sich nach der Aktivierung der zweistufigen Überprüfung zum ersten Mal bei Kaspersky Security Center anmelden, wird das Fenster zur Konfiguration der zweistufigen Überprüfung für Ihr eigenes Benutzerkonto geöffnet.

Stellen Sie sicher, dass auf dem mobilen Gerät eine Authenticator-App installiert ist, bevor Sie die zweistufige Überprüfung für Ihr Konto konfigurieren.

Stellen Sie mithilfe externer Zeitquellen sicher, dass die Uhrzeit auf dem Gerät mit der Authenticator-App und die Uhrzeit auf dem Gerät mit dem Administrationsserver mit der UTC-Zeit synchronisiert sind.

So konfigurieren Sie die zweistufige Überprüfung für Ihr Konto:

1. Generieren Sie mithilfe der Authenticator-App auf dem mobilen Gerät einen einmaligen Sicherheitscode. Führen Sie dazu eine der folgenden Maßnahmen durch:

   - Geben Sie den geheimen Schlüssel manuell in die Authenticator-App ein.

   - Klicken Sie auf **QR-Code anzeigen** und scannen Sie den QR-Code mithilfe der Authenticator-App.

   Auf dem Mobilgerät wird ein Sicherheitscode angezeigt.

2. Geben Sie im Fenster zur Konfiguration der zweistufigen Überprüfung den Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie anschließend auf **Überprüfen und anwenden**.

Die zweistufige Überprüfung ist für Ihr Konto konfiguriert. Sie können entsprechend Ihren Rechten auf den Administrationsserver zugreifen.

Zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren (MMC-basiert)

Wenn Sie sich nach der Aktivierung der zweistufigen Überprüfung zum ersten Mal bei Kaspersky Security Center anmelden, wird das Fenster zur Konfiguration der zweistufigen Überprüfung für Ihr eigenes Benutzerkonto geöffnet.

Stellen Sie sicher, dass auf dem mobilen Gerät eine Authenticator-App installiert ist, bevor Sie die zweistufige Überprüfung für Ihr Konto konfigurieren. Stellen Sie mithilfe externer Zeitquellen sicher, dass die Uhrzeit auf dem Gerät mit der Authenticator-App und die Uhrzeit auf dem Gerät mit dem Administrationsserver mit der UTC-Zeit synchronisiert sind.

So konfigurieren Sie die zweistufige Überprüfung für Ihr Konto:

1. Generieren Sie mithilfe der Authenticator-App auf dem mobilen Gerät einen einmaligen Sicherheitscode. Führen Sie dazu eine der folgenden Maßnahmen durch:

   - Geben Sie den geheimen Schlüssel manuell in die Authenticator-App ein.
   - Scannen Sie den QR-Code mithilfe der Authenticator-App.

   Auf dem Mobilgerät wird ein Sicherheitscode angezeigt.

2. Geben Sie im Fenster zur **Zweistufige Überprüfung einrichten** den Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie anschließend auf **OK**.

Die zweistufige Überprüfung ist für Ihr Konto konfiguriert. Sie können entsprechend Ihren Rechten auf den Administrationsserver zugreifen.

Neuen geheimen Schlüssel generieren

Sie können nur dann einen neuen geheimen Schlüssel für die zweistufige Überprüfung Ihres Benutzerkontos generieren, wenn Sie sich mithilfe der zweistufigen Überprüfung autorisiert haben.

Um einen neuen geheimen Schlüssel für ein Benutzerkonto zu generieren:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer**.
2. Klicken Sie auf den Namen des Benutzerkontos, für das Sie einen neuen geheimen Schlüssel für die zweistufige Überprüfung generieren möchten.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.
4. Klicken Sie auf der Registerkarte **Schutz des Benutzerkontos** auf den Link **Neuen geheimen Schlüssel generieren**.
5. Geben Sie im angezeigten Fenster zur zweistufigen Überprüfung einen neuen Sicherheitsschlüssel an, der von der Authenticator-App generiert wird.
6. Klicken Sie auf **Überprüfen und anwenden**.

Für den Benutzer wird ein neuer geheimer Schlüssel generiert.

Wenn Sie das Mobilgerät verlieren, können Sie auf einem anderen Mobilgerät eine Authenticator-App installieren und einen neuen geheimen Schlüssel generieren, um den Zugriff auf die Kaspersky Security Center Web Console wiederherzustellen.

Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten

Um die Zugriffssicherheit von Kaspersky Security Center Web Console weiter zu verbessern, können Sie verhindern, dass neue Benutzer die zweistufige Überprüfung für sich selbst einrichten.

Bei aktivierter Option kann ein Benutzer, für den die zweistufige Überprüfung deaktiviert ist (z B. ein neuer Domänenadministrator) die zweistufige Überprüfung nicht für sich selbst konfigurieren. Auf diese Weise kann ein solcher Benutzer ohne Zustimmung eines weiteren Administrators von Kaspersky Security Center, für den die Zwei-Faktor-Authentifikation bereits aktiviert wurde, nicht am Administrationsserver authentifiziert werden und sich nicht an der Kaspersky Security Center Web Console anmelden.

Diese Option ist verfügbar, wenn die Zweistufige Überprüfung für alle Benutzer aktiviert ist.

So verbieten Sie neuen Benutzern, die zweistufige Überprüfung für sich selbst einzurichten:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktivieren Sie im Eigenschaftenfenster auf der Registerkarte **Sicherheit für die Authentifizierung** den Umschalter **Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten**.

Diese Option wirkt sich nicht auf Benutzerkonten aus, die zu den Ausnahmen für die zweistufigen Überprüfung hinzugefügt wurden.

Um einem Benutzer mit deaktivierter zweistufiger Überprüfung den Zugriff auf die Kaspersky Security Center Web Console zu gewähren, deaktivieren Sie vorübergehend die Option **Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten**, fordern Sie den Benutzer auf, die zweistufige Überprüfung zu aktivieren, und aktivieren Sie anschließend die Option wieder.

Benutzer nach der Installation des Administrationsagenten zum Linux-Gerätebesitzer ernennen

So erlauben Sie dem Benutzer, sich als Linux-Gerätebesitzer zu registrieren:

1. Gehen Sie in der Kaspersky Security Center Web Console zu **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete**.

   Die Liste der Installationspakete wird geöffnet.

2. Klicken Sie auf das Installationspaket des Administrationsagenten.

   Das Eigenschaftenfenster des Installationspakets wird geöffnet.

3. Klicken Sie im Eigenschaftenfenster des Installationspakets auf **Einstellungen** → **Erweitert**.

4. Aktivieren Sie im Abschnitt **Benutzerregistrierung als Gerätebesitzer (nur Linux)** die Option **Ausführen des Tools zur Benutzerregistrierung nach Installation des Administrationsagenten zulassen** und klicken Sie auf **Speichern**.

Das Tool zur Benutzerregistrierung als Gerätebesitzer kann über die Befehlszeile auf dem Client-Gerät ausgeführt werden.

So ernennen Sie einen Benutzer zum Linux-Gerätebesitzer des Client-Geräts:

1. Führen Sie in der Befehlszeile des Client-Geräts den folgenden Befehl aus:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner`

2. Geben Sie bei Aufforderung den Benutzernamen und das Kennwort ein.

   Wenn der Benutzername und das Kennwort in der Antwortdatei oder im Installationspaket des Administrationsagenten enthalten sind, führen Sie in der Befehlszeile des Client-Geräts den folgenden Befehl aus:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended`

Wenn der Benutzer zu einer internen Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen enthalten.

Wenn der Benutzer zu einer Active Directory-Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen und den Domänennamen enthalten.

Wenn für den Benutzer die zweistufige Überprüfung aktiviert ist, müssen Sie das zeitbasierte Einmalkennwort (TOTP) aus der App eingeben.

Der Benutzer wird als Gerätebesitzer registriert.

Löschen eines Benutzers oder einer Sicherheitsgruppe

Sie können nur interne Benutzer oder interne Sicherheitsgruppen löschen.

So löschen Sie einen Benutzer oder eine Sicherheitsgruppe:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** oder **Gruppen** aus.

2. Aktivieren Sie das Kontrollkästchen neben dem Benutzer oder neben der Sicherheitsgruppe, den oder die Sie entfernen möchten.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **OK**.

   Der Benutzer oder die Sicherheitsgruppe ist gelöscht.

Kennwort eines Benutzerkontos ändern

Sie müssen möglicherweise das Kennwort für Ihr eigenes Konto oder für ein anderes Benutzerkonto ändern, wenn das aktuelle Kennwort bald abläuft oder Sie es durch ein sichereres ersetzen möchten.

Das Kennwort muss den folgenden Regeln entsprechen:

- Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Ziffern (0–9)
  - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

Kennwort des eigenen Benutzerkontos ändern

So ändern Sie das Kennwort für Ihr Benutzerkonto:

1. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Kennwort ändern**.
2. Geben Sie das aktuelle Kennwort ein und geben Sie anschließend das neue Kennwort für die Verbindung mit Kaspersky Security Center an.

   Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .
3. Wenn Ihr Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im Fenster **Schutz des Benutzerkontos** die Anmeldeinformationen Ihres eigenen Benutzerkontos oder eines Benutzerkontos an, das über die Berechtigung Objekt-ACL ändern für den Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" verfügt.
4. Wenn die zweistufige Überprüfung für das Konto aktiviert ist, das Sie im vorherigen Schritt verwendet haben, geben Sie den Sicherheitscode ein, der von der Authenticator-App auf dem mobilen Gerät generiert wurde.

Kennwort eines internen Benutzerkontos ändern

So ändern Sie das Kennwort eines internen Benutzerkontos:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf den Namen des Benutzerkontos, das Sie bearbeiten möchten.
3. Klicken Sie in dem neuen Fenster mit den Benutzereinstellungen auf der Registerkarte **Allgemein** auf die Schaltfläche **Kennwort ändern**.
4. Geben Sie ein neues Kennwort an, dass für die Verbindung des Benutzers mit Kaspersky Security Center verwendet wird.

   Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .
5. Bei Bedarf können Sie die Option **Der Benutzer muss bei der ersten Anmeldung das Kennwort ändern** aktivieren, um bei der nächsten Authentifizierung eines Benutzers eine Kennwortänderung zu erzwingen.

6. Wenn das Benutzerkonto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im Fenster **Schutz des Benutzerkontos** die Anmeldeinformationen des Benutzerkontos an, das über die Berechtigung Objekt-ACL ändern für den Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" verfügt.

7. Wenn die zweistufige Überprüfung für das Konto aktiviert ist, das Sie im vorherigen Schritt verwendet haben, geben Sie den Sicherheitscode ein, der von der Authenticator-App auf dem mobilen Gerät generiert wurde.

Konfigurieren der Optionen zum Ändern eines Kennworts mithilfe von Server-Flags

Sie können das Tool "klscflag" verwenden, um die Kennwortänderung mit den folgenden Befehlen zu konfigurieren:

- Konfiguration des Zeitraums für die Kennwort-Rotation (Flag `LP_SplPwdChangePeriodDays`)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <Rotationszeitraum>
  ```

  Wobei `<Rotationszeitraum>` für die Zeitspanne in Tagen steht, nach der das Benutzerkennwort abläuft. Mögliche Werte: 0 – 730. Wenn der Parameter den Wert "0" besitzt, ist die Rotation des Kennworts deaktiviert.

- Konfigurieren der Zeitspanne für die vorherige Warnung über eine erforderliche Kennwortänderung (Flag `LP_SplPwdChangeNotificationHours`)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <Warnungszeitraum>
  ```

  Wobei `<Warnungszeitraum>` für die Zeitspanne in Stunden steht, bevor das Benutzerkennwort abläuft. Während dieser Zeitspanne wird eine Benachrichtigung über die erforderliche Kennwortänderung angezeigt. Mögliche Werte: 0 – 17520. Wenn der Parameter den Wert "0" besitzt, beträgt der Warnungszeitraum 25 Prozent des Zeitraums für die Kennwort-Rotation.

- Festlegen des Standardwerts für die Option **Der Benutzer muss bei der ersten Anmeldung das Kennwort ändern** (Flag `LP_SplPwdForceChange`)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <Wert>
  ```

  Mögliche Werte des Flags `<Wert>`:

  `1` – Die Option **Der Benutzer muss bei der ersten Anmeldung das Kennwort ändern** ist aktiviert.

  `0` – Die Option **Der Benutzer muss bei der ersten Anmeldung das Kennwort ändern** ist deaktiviert.

Um den aktuellen Wert eines Flags anzuzeigen, führen Sie den folgenden Befehl aus:

```
klscflag.exe -fget -pv .core/.independent -s KLLIM -n <Flag> -t d
```

Wobei `<Flag>` dem Flag `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` oder `LP_SplPwdForceChange` entspricht.

Benutzerrollen erstellen

So erstellen Sie eine Benutzerrolle:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Geben Sie im folgenden Fenster **Neuer Rollenname** den Namen der neuen Rolle ein.

4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.

5. Ändern Sie im folgenden Fenster für Rolleneigenschaften die Einstellungen der Rolle:

   - Bearbeiten Sie auf der Registerkarte **Allgemein** den Rollennamen.

     Sie können den Namen einer vordefinierten Rolle nicht bearbeiten.

   - Bearbeiten Sie auf der Registerkarte **Einstellungen** den Rollenbereich und die mit der Rolle verknüpften Richtlinien und Profile.

   - Bearbeiten Sie auf der Registerkarte **Zugriffsrechte** die Berechtigungen für den Zugriff auf die Kaspersky-Anwendungen.

6. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die neue Rolle wird in der Liste der Benutzerrollen angezeigt.

Benutzerrollen bearbeiten

So bearbeiten Sie eine Benutzerrolle:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.

2. Klicken Sie auf den Namen der Rolle, die Sie bearbeiten möchten.

3. Ändern Sie im folgenden Fenster für Rolleneigenschaften die Einstellungen der Rolle:

   - Bearbeiten Sie auf der Registerkarte **Allgemein** den Rollennamen.

     Sie können den Namen einer vordefinierten Rolle nicht bearbeiten.

   - Bearbeiten Sie auf der Registerkarte **Einstellungen** den Rollenbereich und die mit der Rolle verknüpften Richtlinien und Profile.

   - Bearbeiten Sie auf der Registerkarte **Zugriffsrechte** die Berechtigungen für den Zugriff auf die Kaspersky-Anwendungen.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die aktualisierte Rolle wird in der Liste der Benutzerrollen angezeigt.

Gültigkeitsbereich einer Benutzerrolle bearbeiten

Ein *Benutzerrollenbereich* ist eine Kombination von Benutzern und Administrationsgruppen. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

Um Benutzer, Sicherheitsgruppen und Administrationsgruppen zum Bereich einer Benutzerrolle hinzuzufügen, können Sie eine der folgenden Methoden anwenden:

Methode 1:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** oder **Gruppen** aus.

2. Aktivieren Sie die Kontrollkästchen neben den Benutzern oder Sicherheitsgruppen, die Sie dem Bereich der Benutzerrolle hinzufügen möchten.

3. Klicken Sie auf die Schaltfläche **Rolle zuordnen**.

   Der Assistent zum Zuweisen einer Rolle wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

4. Wählen Sie im Schritt **Rolle auswählen** des Assistenten die Benutzerrolle aus, die Sie zuweisen möchten.

5. Wählen Sie in dem Schritt **Bereich definieren** die Administrationsgruppe aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.

6. Klicken Sie auf die Schaltfläche **Rolle zuordnen**, um das Fenster zu schließen.

Die ausgewählten Benutzer oder Sicherheitsgruppen und die ausgewählte Administrationsgruppe werden dem Bereich der Benutzerrolle hinzugefügt.

Methode 2:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.

2. Klicken Sie auf den Namen der Rolle, für die Sie den Bereich definieren möchten.

3. Wählen Sie im folgenden Eigenschaftenfenster der Rolle die Registerkarte **Einstellungen** aus.

4. Klicken Sie im Abschnitt **Bereich der Rolle** auf **Hinzufügen**.

   Der Assistent zum Zuweisen einer Rolle wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

5. Wählen Sie im Schritt **Bereich definieren** die Administrationsgruppe aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.

6. Wählen Sie im Schritt **Benutzer auswählen** die Benutzer und Sicherheitsgruppen aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.

7. Klicken Sie auf die Schaltfläche **Rolle zuordnen**, um das Fenster zu schließen.

8. Klicken Sie auf die Schaltfläche **Schließen** (⨯), um das Eigenschaftenfenster der Rolle zu schließen.

Die ausgewählten Benutzer oder Sicherheitsgruppen und die ausgewählte Administrationsgruppe werden dem Bereich der Benutzerrolle hinzugefügt.

Methode 3:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Zugriffsrechte** das Kontrollkästchen neben dem Namen des Benutzers oder der Sicherheitsgruppe, die Sie dem Benutzerrollenbereich hinzufügen möchten, und klicken Sie dann auf die Schaltfläche **Rollen**.

   Sie können nur einzelne Benutzer oder Sicherheitsgruppen auswählen. Wenn Sie mehr als ein Element auswählen, wird die Schaltfläche **Rollen** deaktiviert.

3. Wählen Sie im Fenster **Rollen** die Benutzerrolle aus, die Sie zuweisen möchten, wenden Sie dann die Änderungen an und speichern Sie sie.

   Die ausgewählten Benutzer oder Sicherheitsgruppen werden in den Geltungsbereich der Benutzerrolle aufgenommen.

Benutzerrollen löschen

So löschen Sie eine Benutzerrolle:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.
2. Aktivieren Sie die Kontrollkästchen neben dem Namen, den Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Die Benutzerrolle ist gelöscht.

Richtlinienprofile mit Rollen verbinden

Sie können Benutzerrollen mit Richtlinienprofilen verbinden. In diesem Fall basiert die Aktivierungsregel für dieses Richtlinienprofil auf der Rolle: das Richtlinienprofil wird für einen Benutzer aktiv, der über die festgelegte Rolle verfügt.

Beispielsweise verbietet die Richtlinie auf allen Geräten der Administrationsgruppe Programme zur GPS-Navigation. GPS-Navigation sind nur auf einem einzigen Gerät in der Administrationsgruppe "Benutzer" erforderlich, dem Gerät, dessen Inhaber als Kurier beschäftigt ist. In diesem Fall können Sie seinem Inhaber eine "Kurier"-Rolle zuweisen und dann einen Richtlinienprofil erstellen, das die Ausführung von GPS-Navigationssoftware nur auf den Geräten erlaubt, deren Inhabern die "Kurier"-Rolle zugewiesen ist. Alle anderen Richtlinieneinstellungen bleiben erhalten. Nur der Benutzer mit der Rolle "Kurier" hat die Erlaubnis, GPS-Navigationssoftware auszuführen. Wenn später einem weiteren Mitarbeiter die "Kurier"-Rolle zugewiesen wird, darf der neue Mitarbeiter ebenfalls Navigationssoftware auf den Geräten Ihrer Organisation ausführen. Das Ausführen von GPS-Navigationssoftware ist auf anderen Geräten in derselben Administrationsgruppe weiterhin verboten.

Um eine Rolle mit einem Richtlinienprofil zu verbinden, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.
2. Klicken Sie auf den Namen und die Rolle, die Sie mit einem Richtlinienprofil verbinden möchten.

   Das Fenster "Rolleneigenschaften" wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.
3. Wählen Sie die Registerkarte **Einstellungen** aus und scrollen Sie nach unten zum Abschnitt **Richtlinien und Profile**.
4. Klicken Sie auf die Schaltfläche **Bearbeiten**.
5. Um die Rolle mit einem der folgenden Profile zu verbinden, gehen Sie wie folgt vor:

   - **Vorhandenes Richtlinienprofil**: Klicken Sie auf das Chevron-Symbol (>) neben dem entsprechenden Richtliniennamen und aktivieren Sie dann das Kontrollkästchen neben dem Profil, mit dem Sie die Rolle verbinden möchten.
   - **Neues Richtlinienprofil**:

     a. Aktivieren Sie das Kontrollkästchen neben der Richtlinie, für die Sie ein Profil erstellen möchten.

     b. Klicken Sie auf die Schaltfläche **Neues Richtlinienprofil**.

     c. Geben Sie den Namen des neuen Profils ein und passen Sie seine Einstellungen an.

     d. Klicken Sie auf die Schaltfläche **Speichern**.

     e. Aktivieren Sie das Kontrollkästchen neben dem neuen Profil.
6. Klicken Sie auf die Schaltfläche **Einer Rolle zuordnen**.

Das Profil wird mit der Rolle verbunden und in den Eigenschaften der Rolle angezeigt. Das Profil wird automatisch für alle Geräte übernommen, deren Inhabern die Rolle zugewiesen ist.

Ausdehnen von Benutzerrollen auf sekundäre Administrationsserver

Standardmäßig sind die Listen der Benutzerrollen des primären und der sekundären Administrationsserver voneinander unabhängig. Sie können die Anwendung so anpassen, dass die auf dem primären Administrationsserver erstellten Benutzerrollen automatisch auf alle sekundären Administrationsserver verteilt werden. Die Benutzerrollen können auch von einem sekundären Administrationsserver auf dessen eigene sekundäre Administrationsserver verteilt werden.

Um Benutzerrollen vom primären Administrationsserver auf die sekundären Administrationsserver zu verteilen:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wechseln Sie zum Abschnitt **Hierarchie der Administrationsserver**.

3. Aktivieren Sie die Option **Liste mit Rollen an sekundäre Administrationsserver weiterleiten** und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Die Anwendung kopiert die Benutzerrollen des primären Administrationsservers auf die sekundären Administrationsserver.

Wenn die Option **Liste mit Rollen an sekundäre Administrationsserver weiterleiten** aktiviert ist und die Benutzerrollen verteilt werden, können sie auf den sekundären Administrationsservern nicht geändert oder gelöscht werden. Wenn Sie auf dem primären Administrationsserver eine neue Rolle erstellen oder eine bestehende ändern, werden die Änderungen automatisch auf die sekundären Administrationsserver kopiert. Wenn Sie auf dem primären Administrationsserver eine Benutzerrolle löschen, verbleibt diese Rolle danach auf den sekundären Administrationsservern, kann aber geändert oder gelöscht werden.

Die vom primären Administrationsserver an die sekundären Administrationsserver weitergeleiteten Rollen werden durch grüne Häkchen (✓) markiert. Diese Rollen können auf dem sekundären Administrationsserver nicht bearbeitet werden.

Wenn Sie eine Rolle auf dem primären Administrationsserver erstellen, während auf seinem sekundären Administrationsserver eine Rolle mit demselben Namen vorhanden ist, wird die neue Rolle auf den sekundären Administrationsserver kopiert und der Rollenname um einen Index erweitert, z. B. ~~1 oder ~~2 (der Index kann eine Zufallszahl sein).

Wenn Sie die Option **Liste mit Rollen an sekundäre Administrationsserver weiterleiten** deaktivieren, verbleiben alle Benutzerrollen auf den sekundären Administrationsservern, werden dabei jedoch von jeder Rolle auf dem primären Administrationsserver unabhängig. Nachdem sie unabhängig wurden, können die Benutzerrollen auf den sekundären Administrationsservern geändert oder gelöscht werden.

Kennwort des Benutzerkontos ändern

Sie können das Kennwort eines lokalen Benutzerkontos ändern. Dies kann nützlich sein, wenn ein Benutzer das Kennwort seines lokalen Kontos vergisst oder wenn eine geplante Kennwortänderung durchgeführt wird.

Die Kennwortänderung ist auch dann wirksam, wenn der Benutzer nicht beim Konto angemeldet ist. Sie können auch das Kennwort für das lokale Root-Konto ändern.

Diese Aufgabe kann nur auf Linux-Geräten ausgeführt werden.

So ändern Sie das Kennwort des lokalen Kontos für ausgewählte Geräte:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.

3. Wählen Sie im Feld **Aufgabentyp** den die Option **Kennwort des Benutzerkontos ändern (nur Linux)** aus.

4. Wählen Sie eine der folgenden Varianten aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

     Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

   - **Aufgabe einer Geräteauswahl zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

     Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

   Die Aufgabe *Kennwort des Benutzerkontos ändern (nur Linux)* wird für die angegebenen Geräte erstellt. Wenn Sie Option **Aufgabe einer Administrationsgruppe zuweisen** ausgewählt haben, ist die Aufgabe eine Gruppenaufgabe.

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

   Die verfügbaren Einstellungen hängen von der im vorherigen Schritt ausgewählten Option ab.

6. Geben Sie im Schritt **Geben Sie den Namen des Benutzerkontos und das neue Kennwort an** die folgenden Einstellungen an:

   - Geben Sie im Feld **Name des Benutzerkontos** den Namen des Kontos an, für welches Sie das Kennwort ändern möchten.

   - Geben Sie im Feld **Neues Kennwort** das Kennwort an, das Sie für das im vorherigen Feld angegebene Benutzerkonto festlegen möchten.

     Wenn Sie die eingegebenen Zeichen sehen möchten, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie sie gedrückt.

   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Dies ist ein Einmalkennwort (der Benutzer muss das Kennwort nach dem ersten Anmelden ändern)**.

     - **Dies ist ein Einmalkennwort (der Benutzer muss das Kennwort nach dem ersten Anmelden ändern)**

       Wenn dieses Kontrollkästchen aktiviert ist, wird der Benutzer nach der ersten Anmeldung aufgefordert, ein neues Kennwort festzulegen.

Wenn dieses Kontrollkästchen deaktiviert ist, wird der Benutzer nach der ersten Anmeldung nicht aufgefordert, ein neues Kennwort festzulegen.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

7. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu beenden.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen, ändern oder bei Bedarf einen Startzeitplan für die Aufgabe konfigurieren.

8. Wählen Sie in der Aufgabenliste die von Ihnen erstellte Aufgabe aus und klicken Sie anschließend auf **Start**.

   Alternativ können Sie warten, bis die Aufgabe nach dem Zeitplan aus den Aufgabeneinstellungen gestartet wird.

Nach Abschluss der Aufgabe zur Kennwortänderung wird das Kennwort für das angegebene lokale Konto auf den ausgewählten Geräten geändert.

Um sicherzustellen, dass die Aufgaben zur Kennwortänderung korrekt ausgeführt werden, muss SELinux auf dem Benutzergerät deaktiviert sein.

Lokale Administratorrechte entziehen

Sie können den Benutzerkonten lokale Administratorrechte entziehen. Dadurch erhalten Sie mehr Kontrolle über die Benutzerkonten. Sie können beispielsweise die lokalen Administratorrechte entziehen, nachdem eine einmalige Zuweisung abgeschlossen wurde.

Beim Ausführen dieser Aufgabe wird überprüft, ob das angegebene lokale Benutzerkonto zu den Gruppen mit lokalen Administratoren gehört. Diese Gruppen werden in den Richtlinieneinstellungen des Administrationsagenten definiert. Sie können die Liste der Gruppen mit lokalen Administratoren in den Richtlinieneinstellungen des Administrationsagenten konfigurieren. Sie können die Liste der privilegierten Benutzerkonten auch mithilfe des **Bericht über privilegierte Gerätenutzer (nur Linux)** überprüfen.

Diese Aufgabe kann nur auf Linux-Geräten ausgeführt werden.

So entziehen Sie die lokalen Administratorrechte auf ausgewählten Geräten:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.

3. Wählen Sie im Feld **Aufgabentyp** die Option **Lokale Administratorrechte widerrufen (nur Linux)**.
4. Wählen Sie eine der folgenden Varianten aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

- **Geräteadressen manuell angeben oder aus Liste importieren**

  Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

  Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Die Aufgabe *Lokale Administratorrechte entziehen (nur Linux)* wird für die angegebenen Geräte erstellt. Wenn Sie die Option **Aufgabe einer Administrationsgruppe zuweisen** ausgewählt haben, ist die Aufgabe eine Gruppenaufgabe.

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

   Die verfügbaren Einstellungen hängen von der im vorherigen Schritt ausgewählten Option ab.

6. Geben Sie in diesem Schritt des Assistenten die folgenden Einstellungen an:

   - Wählen Sie in der Einstellungsgruppe **Ausführungsmodus** den Ausführungsmodus aus:

     - **Lokale Administratorrechte von den aufgelisteten Benutzerkonten widerrufen**

       Wenn diese Option aktiviert ist, werden den angegebenen lokalen Benutzerkonten die lokalen Administratorrechte entzogen.

       Diese Option ist standardmäßig ausgewählt.

     - **Aufgelistete Benutzerkonten vom Widerruf der lokalen Administratorrechte ausschließen**

       Wenn diese Option ausgewählt ist, werden die lokalen Administratorrechte allen lokalen Benutzerkonten außer den angegeben entzogen.

       Diese Variante ist standardmäßig nicht ausgewählt.

- Geben Sie die lokalen Benutzerkonten an:
  - Klicken Sie auf **Hinzufügen**.
  - Führen Sie im nächsten Fenster die folgenden Schritte aus:
    - Geben Sie im Feld **Benutzerkonto-Name** den Namen des lokalen Benutzerkontos an.
    - Wählen Sie in der Einstellungsgruppe **Aktion für das Benutzerkonto** (nur verfügbar, wenn die Option **Lokale Administratorrechte von den aufgelisteten Benutzerkonten widerrufen** ausgewählt ist) eine Aktion aus.
    - **Benutzerkonto beibehalten**

      Wenn diese Option ausgewählt ist, wird das lokale Benutzerkonto nicht gelöscht, nachdem die lokalen Administratorrechte entzogen wurden.

      Diese Option ist standardmäßig ausgewählt.
    - **Benutzerkonto löschen**

      Wenn diese Option ausgewählt ist, wird das lokale Benutzerkonto gelöscht, unabhängig davon, ob es über lokale Administratorrechte verfügt.

      Diese Variante ist standardmäßig nicht ausgewählt.

7. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu beenden.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen, ändern oder bei Bedarf einen Startzeitplan für die Aufgabe konfigurieren.

8. Wählen Sie in der Aufgabenliste die von Ihnen erstellte Aufgabe aus und klicken Sie anschließend auf **Start**.

   Alternativ können Sie warten, bis die Aufgabe nach dem Zeitplan aus den Aufgabeneinstellungen gestartet wird.

Nachdem die Aufgabe zum Entziehen lokaler Administratorrechte abgeschlossen ist, wurden den angegebenen lokalen Benutzerkonten auf den festgelegten Geräten die lokalen Administratorrechte entzogen.

Umgang mit Objekt-Revisionen

Der Abschnitt enthält Informationen über die Arbeit mit den Revisionen des Objekts. Kaspersky Security Center erlaubt eine Nachverfolgung der Änderungen von Objekten. Jedes Mal, wenn Sie die Änderungen des Objektes speichern, wird eine *Revision* erstellt. Jede Revision hat eine Nummer.

Folgende Objekte der Anwendung unterstützen die Arbeit mit Revisionen:

- Eigenschaften des Administrationsservers
- Richtlinien
- Aufgaben
- Administrationsgruppen

- Benutzerkonten
- Installationspakete

Sie können mit den Revisionen von Objekten folgende Aktionen ausführen:

- Eine ausgewählten Revision anzeigen (nur für Richtlinien)
- Ein Rollback der Objektänderungen auf eine ausgewählte Revision durchführen
- Revisionen in einer JSON-Datei speichern (nur für Richtlinien)

Im Eigenschaftenfenster der Objekte, die den Umgang mit Revisionen unterstützen, wird im Abschnitt **Revisionsverlauf** eine Liste der Objektrevisionen mit den folgenden Informationen angezeigt:

- **Revision** – Nummer der Revision des Objekts
- **Uhrzeit** – Datum und Uhrzeit der Objektänderung
- **Benutzer** – Name des Benutzers, der das Objekt geändert hat
- **IP-Adresse des Benutzergeräts** – IP-Adresse des Geräts, von dem aus das Objekt geändert wurde.
- **IP-Adresse der Web Console** – IP-Adresse der Kaspersky Security Center Web Console, mit der das Objekt geändert wurde.
- **Aktion** – Aktion, die auf das Objekt angewendet wurde
- **Beschreibung** – Informationen zu den Änderungen der Objekteinstellungen für diese Revision

  Standardmäßig ist die Beschreibung der Revision des Objekts nicht ausgefüllt. Um eine Beschreibung der Revision hinzuzufügen, wählen Sie die gewünschte Revision aus und klicken Sie auf die Schaltfläche **Beschreibung bearbeiten**. Geben Sie im folgenden Fenster einen Text zur Beschreibung der Revision ein.

Objekte auf eine frühere Version zurück rollen

Falls erforderlich können Sie an einem Objekt vorgenommene Änderungen zurücksetzen. Beispielsweise kann es erforderlich sein, die Einstellungen der Richtlinie auf den Zustand eines bestimmten Datums zurückzusetzen.

So setzen Sie e an einem Objekt vorgenommene Änderungen zurück:

1. Wählen Sie im Eigenschaftenfenster des Objekts die Registerkarte **Revisionsverlauf** aus.
2. Wählen Sie in der Liste mit den Revisionen des Objekts die Revision aus, auf deren Stand die Änderungen zurückgesetzt werden sollen.

3. Klicken Sie auf die Schaltfläche **Rollback**.

4. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

   Das Objekt wird auf die ausgewählte Revision zurückgesetzt. In der Liste der Revisionen des Objektes wird ein Eintrag über die ausgeführte Aktion angezeigt. In der Beschreibung der Revision werden die Informationen über die Nummer der Revision angezeigt, auf die Sie das Objekt zurückgesetzt haben.

Das Zurücksetzen von Revisionen ist nur für Richtlinien- und Aufgabenobjekte verfügbar.

Hinzufügen einer Beschreibung der Revision

Kaspersky Security Center erlaubt eine Nachverfolgung der Änderungen von Objekten. Jedes Mal, wenn Sie die Änderungen des Objektes speichern, wird eine Revision erstellt. Jede Revision hat eine Nummer.

Sie können eine Beschreibung für die Revision hinzufügen, damit es künftiger einfacher ist, die gewünschte Revision in der Liste zu finden.

Um eine Beschreibung der Revision hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster des Objekts die Registerkarte **Revisionsverlauf** aus.

2. Wählen Sie in der Liste der Revisionen des Objektes die Revision aus, für die eine Beschreibung hinzugefügt werden soll.

3. Klicken Sie auf die Schaltfläche **Beschreibung bearbeiten**.

   Das Fenster **Beschreibung** wird geöffnet.

4. Geben Sie im Fenster **Beschreibung** einen Text zur Beschreibung der Revision ein.

   Standardmäßig ist die Beschreibung der Revision des Objekts nicht ausgefüllt.

5. Speichern Sie die Beschreibung der Revision.

Der Revision des Objekts wird eine Beschreibung hinzugefügt.

Revision einer Richtlinie anzeigen und speichern

In Kaspersky Security Center können Sie anzeigen, welche Änderungen an einer Richtlinie in einem bestimmten Zeitraum vorgenommen wurden, und Informationen über diese Änderungen in einer Datei speichern.

Anzeige und Speichern einer Richtlinienrevision sind verfügbar, wenn diese Funktionalität durch das entsprechende Verwaltungs-Web-Plug-in unterstützt wird.

So zeigen Sie eine Richtlinienrevision an:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

2. Klicken Sie auf die Richtlinie, deren Revision Sie anzeigen möchten, und gehen Sie dann zum Abschnitt **Revisionsverlauf**.

3. Klicken Sie in der Liste mit den Richtlinienrevisionen auf die Nummer der Revision, die Sie anzeigen möchten.

   Wenn die Revision größer als 10 MB ist, können Sie diese in der Kaspersky Security Center Web Console nicht anzeigen. Sie werden aufgefordert, die ausgewählte Revision in einer JSON-Datei zu speichern.

   Wenn die Revision nicht größer als 10 MB ist, werden die Einstellungen der ausgewählten Richtlinienrevision als Bericht im HTML-Format angezeigt. Der Bericht wird in einem Pop-up-Fenster angezeigt. Daher müssen Sie sicherstellen, dass das Anzeigen von Pop-ups in Ihrem Browser erlaubt ist.

So speichern Sie eine Richtlinienrevision als JSON-Datei:

Wählen Sie in der Liste der Richtlinienrevisionen die Revision aus, die Sie speichern möchten, und klicken Sie dann auf **In Datei speichern**.

Die Revision wird in einer JSON-Datei gespeichert.

Löschen von Objekten

Dieser Abschnitt enthält Informationen über das Löschen von Objekten.

Sie können Objekte löschen, einschließlich der folgenden:

- Richtlinien
- Aufgaben
- Installationspakete
- Virtuelle Administrationsserver
- Benutzer
- Sicherheitsgruppen
- Administrationsgruppen

Um ein Objekt zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie den erforderlichen Bereich in der Kaspersky Security Center Web Console und wählen Sie anschließend das Objekt aus.
2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Löschen**.
3. Klicken Sie im folgenden Fenster auf **OK**, um die Auswahl zu bestätigen.

   Das ausgewählte Objekt wird gelöscht.

Wenn Sie ein Objekt löschen, verbleiben die Informationen darüber in der Datenbank. Die Speicherdauer für Informationen über die gelöschten Objekte ist dieselbe wie die Speicherdauer für Revisionen des Objekts (die empfohlenen Dauer beträgt 90 Tage). Sie können die Speicherdauer nur ändern, wenn Sie über die Berechtigung **zum Ändern** im Berechtigungsbereich **Gelöschte Objekte** verfügen.

Über das Löschen von Client-Geräten

Wenn Sie ein verwaltetes Gerät aus einer Administrationsgruppe löschen, verschiebt die Anwendung das Gerät in die Gruppe "Nicht zugeordnete Geräte". Nach dem Löschen des Geräts verbleiben der installierte Administrationsagent und die Kaspersky-Sicherheitsanwendungen, wie Kaspersky Endpoint Security, auf dem Gerät.

Kaspersky Security Center geht mit den Geräten in der Gruppe "Nicht zugeordnete Geräte" gemäß den folgenden Regeln um:

- Wenn Sie Verschiebungsregeln für Geräte konfiguriert haben und ein Gerät die Kriterien einer Verschiebungsregel erfüllt, wird das Gerät automatisch gemäß dieser Regel in eine Administrationsgruppe verschoben.

- Das Gerät wird in der Gruppe "Nicht zugeordnete Geräte" gespeichert und entsprechend der Aufbewahrungsregeln für Geräte automatisch aus der Gruppe entfernt.

  Die Aufbewahrungsregeln für Geräte wirken sich nicht auf Geräte aus, in denen Laufwerke mit vollständiger Festplattenverschlüsselung verschlüsselt sind. Solche Geräte werden nicht automatisch gelöscht, sondern können nur manuell gelöscht werden. Wenn Sie ein Gerät mit einem verschlüsselten Laufwerk löschen müssen, entschlüsseln Sie zuerst das Laufwerk und löschen Sie anschließend das Gerät.

  > Wenn Sie ein Gerät mit einem verschlüsselten Laufwerk löschen, werden auch die zum Entschlüsseln des Laufwerks erforderlichen Daten gelöscht. Wenn Sie im Bestätigungsfenster, das sich öffnet, wenn Sie solche Geräte löschen (entweder aus der Gruppe **Nicht zugeordnete Geräte** oder aus der Gruppe **Verwaltete Geräte**), das Kontrollkästchen **Ich kenne das Risiko und möchte die ausgewählten Geräte löschen** aktivieren, geben Sie an, dass Sie von der anschließenden Datenlöschung Kenntnis haben.

  Um das Laufwerk zu entschlüsseln, müssen die folgenden Bedingungen erfüllt sein:

  - Das Gerät wird erneut mit dem Administrationsserver verbunden, um die zum Entschlüsseln des Laufwerks erforderlichen Daten wiederherzustellen.

  - Der Benutzer des Geräts merkt sich das Kennwort zum Entschlüsseln.

  - Die Sicherheitsanwendung, mit der das Laufwerk verschlüsselt wurde (z. B. Kaspersky Endpoint Security für Windows), ist weiterhin auf dem Gerät installiert.

  Wenn das Laufwerk mittels Kaspersky-Festplattenverschlüsselung verschlüsselt wurde, können Sie auch versuchen, die Daten mithilfe des Wiederherstellungs-Tools FDERT wiederherzustellen.

> Wenn Sie ein Gerät mit verschlüsselten Laufwerken in einer VDI-Umgebung besitzen, werden die Informationen auf dem verschlüsselten Laufwerk gelöscht, nachdem Sie das Gerät gelöscht haben.

Wenn Sie ein Gerät manuell aus der Gruppe "Nicht zugeordnete Geräte" löschen, entfernt die Anwendung das Gerät aus der Liste. Nach dem Löschen des Geräts verbleiben etwaige installierte Kaspersky -Anwendungen auf dem Gerät. Wenn das Gerät für den Administrationsserver weiterhin sichtbar ist und Sie die regelmäßige Netzwerkabfrage konfiguriert haben, erkennt Kaspersky Security Center das Gerät während der Netzwerkabfrage und fügt es erneut der Gruppe "Nicht zugeordnete Geräte" hinzu. Daher ist es sinnvoll, ein Gerät nur dann manuell zu löschen, wenn es für den Administrationsserver nicht mehr sichtbar ist.

Kaspersky Security Network (KSN)

In diesem Abschnitt wird die Verwendung der Infrastruktur der Online-Dienste von Kaspersky Security Network (KSN) beschrieben. Er enthält Informationen über KSN sowie Anleitungen zur Aktivierung von KSN, zur Konfiguration des Zugriffs auf KSN und über die Statistiken der Verwendung des KSN-Proxyservers.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Über KSN

Das Kaspersky Security Network (KSN) ist eine Infrastruktur von Online-Diensten, die Zugriff auf die aktuelle Wissensdatenbank von Kaspersky bietet, in der Informationen über die Reputation der Dateien, Web-Ressourcen und Programme enthalten sind. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. Mit KSN können aus den Kaspersky-Reputations-Datenbanken Informationen über die Anwendungen abgerufen werden, die auf den verwalteten Geräten installiert sind.

Kaspersky Security Center unterstützt die folgenden Infrastrukturlösungen:

- *KSN* ist eine Lösung, mit der Sie Informationen mit dem Kaspersky Security Network austauschen können. Wenn Sie an KSN teilnehmen, stimmen Sie zu, dass Informationen über die Ausführung der auf den Client-Geräten installierten Kaspersky-Anwendungen, die von Kaspersky Security Center verwaltet werden, automatisch an Kaspersky übertragen werden. Die Übertragung von Informationen erfolgt gemäß den aktuellen Einstellungen für den Zugriff auf KSN. Kaspersky-Analysten analysieren zusätzlich erhaltene Informationen und nehmen sie in die Reputations- und Statistikdatenbanken von Kaspersky Security Network auf. Kaspersky Security Center verwendet standardmäßig diese Lösung.

- *Kaspersky Private Security Network (KPSN)* ist eine Lösung, die es Benutzern von Geräten mit installierten Kaspersky-Anwendungen ermöglicht, Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network und andere statistische Daten zu erhalten, ohne Daten von ihren eigenen Geräten an Global KSN zu senden. KPSN richtet sich an Unternehmenskunden, die aus einem der folgenden Gründe nicht an Kaspersky Security Network teilnehmen können:

  - Die Benutzergeräte haben keine Internetverbindung.

  - Die Übermittlung von Daten an einen Punkt außerhalb des Landes oder außerhalb des lokalen Unternehmensnetzwerks ist gesetzlich oder aufgrund von Sicherheitsrichtlinien des Unternehmens untersagt.

  Sie können die Zugriffseinstellungen von Kaspersky Private Security Network im Abschnitt **KSN Proxy-Einstellungen** des Eigenschaftenfensters des Administrationsservers einstellen.

Die Programm fordert Sie auf, während der Ausführung des Schnellstartassistenten eine Verbindung zu KSN herzustellen. Sie können während der Ausführung des Programms jederzeit mit der Verwendung von KSN beginnen oder auf KSN verzichten.

Sie verwenden KSN gemäß der KSN-Erklärung, die Sie lesen und akzeptieren, wenn Sie KSN aktivieren. Wird die KSN-Erklärung aktualisiert, so wird sie Ihnen bei einem Upgrade der Version des Administrationsservers angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, verwenden Sie KSN weiterhin gemäß der vorherigen Version der KSN-Erklärung, die Sie zuvor akzeptiert haben.

Wenn KSN aktiviert ist, prüft Kaspersky Security Center, ob auf die KSN-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Dies ist notwendig, um sicherzustellen, dass das Sicherheitsniveau für die verwalteten Geräte beibehalten wird.

Vom Administrationsserver verwaltete Client-Geräte interagieren mithilfe des KSN-Proxyservers mit KSN. Der KSN-Proxyserver bietet folgende Möglichkeiten:

- Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen.
- Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Die Einstellungen des KSN-Proxyservers können Sie im Abschnitt **KSN Proxy-Einstellungen** im Eigenschaftenfenster des Administrationsservers ändern.

Zugriff auf KSN einrichten

Sie können den Zugriff auf Kaspersky Security Network (KSN) auf dem Administrationsserver und auf einem Verteilungspunkt anpassen.

Um den Zugriff des Administrationsservers auf KSN einzurichten, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.

3. Setzen Sie den Schalter auf **KSN Proxy auf dem Administrationsserver aktivieren Aktiviert**.

   Wenn diese Option aktiviert ist, sendet der KSN-Proxyserver Daten an KSN, um die Effizienz der Komponenten von Kaspersky Security Center zu erhöhen und die Leistung der Kaspersky-Anwendungen zu verbessern. Die Übertragung von Daten der Client-Geräte an KSN wird durch die Richtlinie von Kaspersky Endpoint Security vorgegeben, die auf den Client-Geräten angewendet wird. Wenn das Kontrollkästchen deaktiviert ist, werden keine Daten vom Administrationsserver und von Client-Geräten über Kaspersky Security Center an KSN übertragen. In diesem Fall können die Client-Geräte Daten entsprechend ihrer Einstellungen direkt an KSN übertragen (nicht über Kaspersky Security Center). Die auf den Client-Geräten geltende Richtlinie für Kaspersky Endpoint Security bestimmt, welche Daten diese Geräte direkt (nicht über Kaspersky Security Center) an KSN senden.

4. Stellen Sie den Umschalter auf die Position **Kaspersky Security Network verwenden Aktiviert**.

   Wenn diese Option aktiviert ist, senden Client-Geräte die Ergebnisse der Patch-Installation an Kaspersky. Wenn Sie diese Option aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.

   Wenn Sie KPSN verwenden, stellen Sie den Umschalter auf die Position **Kaspersky Private Security Network verwenden Aktiviert** und klicken Sie auf die Schaltfläche **Datei mit KSN Proxy-Einstellungen wählen**, um die Einstellungen für KPSN herunterzuladen (Dateien mit den Erweiterungen pkcs7 und pem). Nach dem Herunterladen der Einstellungen werden in der Benutzeroberfläche die Bezeichnung des Providers, die Kontaktdaten des Providers und das Erstellungsdatum der Datei mit Einstellungen von KPSN angezeigt.

Wenn Sie KPSN aktivieren, achten Sie auf die Verteilungspunkte, die so konfiguriert wurden, dass sie KSN-Anfragen direkt an Cloud-KSN versenden. Verteilungspunkte mit installiertem Administrationsagent Version 11 (oder früher) senden weiterhin KSN-Anfragen an Cloud-KSN. Um die Verteilungspunkte so anzupassen, dass KSN-Anfragen an KPSN gesendet werden, aktivieren Sie für jeden Verteilungspunkt die Option **KSN-Anfragen an den Administrationsserver weiterleiten**. Sie können diese Option in den Eigenschaften des Verteilungspunkts oder in der Richtlinie des Administrationsagenten aktivieren.

Wenn Sie den Umschalter in die Position **Kaspersky Private Security Network verwenden Aktiviert** stellen, erscheint eine Nachricht mit Details zu KPSN.

Die folgenden Kaspersky-Anwendungen unterstützten KPSN:

- Kaspersky Security Center
- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

Wenn Sie KPSN in Kaspersky Security Center aktivieren, erhalten diese Programme Informationen zur Unterstützung von KPSN. Im Unterabschnitt **Kaspersky Security Network** des Abschnitts **Erweiterter Schutz** wird im Fenster "Einstellungen" die Information zum ausgewählten KSN-Anbieter angezeigt: Entweder KSN oder KPSN.

Wenn Sie für die Arbeit mit KPSN ältere Programmversionen als Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 oder Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent verwenden, ist es empfehlenswert, die sekundären Administrationsserver zu verwenden, für welche die Nutzung von KPSN nicht konfiguriert ist.

Kaspersky Security Center sendet keine statistischen Daten an Kaspersky Security Network, wenn im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN Proxy-Einstellungen** die Option "KPSN" konfiguriert ist.

5. Wenn Sie die Proxyserver-Einstellungen in den Eigenschaften des Administrationsservers angepasst haben, aber Ihre Netzwerkarchitektur eine direkte Verwendung von KPSN erfordert, aktivieren Sie die Option **Proxyserver-Einstellungen beim Verbinden mit KPSN ignorieren**. Andernfalls können Anfragen von den verwalteten Apps KPSN nicht erreichen.

6. Passen Sie die Einstellungen für die Verbindung des Administrationsservers mit dem Dienst des KSN-Proxy-Service an:

   - Geben Sie unter **Verbindungseinstellungen** für den **TCP-Port** die Nummer des TCP-Ports an, über den die Verbindung zum KSN-Proxyserver aufgebaut werden soll. Standardmäßig erfolgt die Verbindung zum KSN-Proxyserver über Port 13111.

   - Wenn Sie möchten, dass der Administrationsserver die Verbindung zum KSN-Proxyserver über einen UDP-Port herstellt, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine Portnummer für den **UDP-Port** an. Standardmäßig ist diese Option deaktiviert und der TCP-Port wird verwendet. Wenn diese Option aktiviert wird, ist 15111 der standardmäßige UDP-Port für die Verbindung mit dem KSN-Proxyserver.

   - Wenn die verwalteten Geräte eine Verbindung mit dem Administrationsserver über einen HTTPS-Port herstellen sollen, aktivieren Sie die Option **HTTPS verwenden** und geben Sie anschließend im Feld **HTTPS über Port** eine Portnummer an. Standardmäßig ist diese Option deaktiviert und der TCP-Port wird verwendet. Wenn diese Option aktiviert wird, ist 17111 der standardmäßige HTTPS-Port für die Verbindung mit dem KSN-Proxyserver.

7. Stellen Sie den Umschalter auf die Position **Sekundäre Administrationsserver über den primären Administrationsserver mit KSN verbinden Aktiviert**.

   Wenn diese Option aktiviert ist, verwenden die sekundären Administrationsserver den primären Administrationsserver als KSN-Proxyserver. Wenn diese Option deaktiviert ist, verbinden sich die sekundären Administrationsserver selbständig mit KSN. In diesem Fall verwenden die verwalteten Geräte die sekundären Administrationsserver als KSN-Proxyserver.

   > Die sekundären Administrationsserver verwenden den primären Administrationsserver als Proxyserver, wenn in den Eigenschaften der sekundären Administrationsserver im rechten Bereich des Abschnitts **KSN Proxy-Einstellungen** der Umschalter auf die Position **KSN Proxy auf dem Administrationsserver aktivieren Aktiviert** gestellt ist.

8. Klicken Sie auf die Schaltfläche **Speichern**.

Daraufhin werden die Einstellungen für den Zugriff auf KSN gespeichert.

Sie können außerdem den Zugriff des Verteilungspunkts auf KSN anpassen, um z. B. die Auslastung des Administrationsservers zu reduzieren. Der Verteilungspunkt, der als KSN-Proxyserver fungiert, sendet KSN-Anfragen von verwalteten Geräten direkt an Kaspersky, ohne den Administrationsserver zu verwenden.

Um den Zugriff des Verteilungspunkts auf Kaspersky Security Network (KSN) einzurichten, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Verteilungspunkt manuell zugewiesen wurde.

2. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

3. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

4. Klicken Sie auf den Namen des Verteilungspunkts, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

5. Aktivieren Sie im Eigenschaftenfenster des Verteilungspunkts, im Abschnitt **KSN Proxy** die Option **KSN Proxy auf dem Verteilungspunkt aktivieren** und aktivieren Sie anschließend die Option **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**.

6. Klicken Sie auf die Schaltfläche **OK**.

Der Verteilungspunkt wird nun als KSN-Proxyserver fungieren.

Verwendung von KSN aktivieren und deaktivieren

So aktivieren Sie die Verwendung von KSN:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.

3. Setzen Sie den Schalter auf **KSN Proxy auf dem Administrationsserver aktivieren Aktiviert**.

Der KSN-Proxyserver ist aktiviert und sendet Daten an KSN, um die Effizienz der Komponenten von Kaspersky Security Center zu erhöhen und die Leistung der Kaspersky-Anwendungen zu verbessern.

1. Aktivieren Sie je nach der von Ihnen verwendeten Infrastruktur-Lösung für KSN die entsprechenden Schalter.

   - Wenn Sie Global KSN verwenden, setzen Sie den Schalter auf **Kaspersky Security Network verwenden Aktiviert**.

     Das Senden von Daten an KSN ist jetzt verfügbar. Wenn Sie diese Option aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.

   - Wenn Sie KPSN verwenden, setzen Sie den Schalter auf **Kaspersky Private Security Network verwenden Aktiviert** und klicken Sie anschließend auf die Schaltfläche **Datei mit KSN Proxy-Einstellungen wählen**, um die Einstellungen für KPSN herunterzuladen (Dateien mit den Erweiterungen pkcs7 und pem). Nach dem Herunterladen der Einstellungen werden in der Benutzeroberfläche die Bezeichnung des Providers, die Kontaktdaten des Providers und das Erstellungsdatum der Datei mit KPSN-Einstellungen angezeigt.

     Wenn Sie den Schalter auf **Kaspersky Private Security Network verwenden Aktiviert** setzen, erscheint eine Nachricht mit Details zu KPSN.

2. Klicken Sie auf **Speichern**.

So deaktivieren Sie die Verwendung von KSN:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.

3. Setzen Sie den Schalter auf **KSN Proxy auf dem Administrationsserver aktivieren Deaktiviert**, um den KSN-Proxy-Dienst zu deaktivieren.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die akzeptierte KSN-Erklärung anzeigen

Wenn Sie Kaspersky Security Network (KSN) aktivieren, müssen Sie die KSN-Erklärung lesen und akzeptieren. Sie können die akzeptierte KSN-Erklärung jederzeit anzeigen.

So zeigen Sie die akzeptierte KSN-Erklärung an:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.

3. Klicken Sie auf den Link **Erklärung zu Kaspersky Security Network anzeigen**.

Im folgenden Fenster können Sie den Text der akzeptierten KSN-Erklärung anzeigen.

Eine aktualisierte KSN-Erklärung akzeptieren

Sie verwenden KSN gemäß der KSN-Erklärung, die Sie lesen und akzeptieren, wenn Sie KSN aktivieren. Wird die KSN-Erklärung aktualisiert, so wird sie Ihnen bei einem Upgrade der Version des Administrationsservers angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, verwenden Sie KSN weiterhin gemäß der Version der KSN-Erklärung, die Sie zuvor akzeptiert haben.

Nach dem Upgrade einer Version des Administrationsservers wird die aktualisierte KSN-Erklärung automatisch angezeigt. Wenn Sie die aktualisierte KSN-Erklärung ablehnen, können Sie diese später erneut anzeigen und akzeptieren.

So zeigen Sie die KSN-Erklärung an und akzeptieren sie anschließend:

1. Klicken Sie auf den Link **Benachrichtigungen anzeigen** in der oberen rechten Ecke des Programmhauptfensters.

   Das Fenster **Benachrichtigungen** wird geöffnet.

2. Klicken Sie auf den Link **Aktualisierte KSN-Erklärung anzeigen**.

   Das Fenster **Update der Erklärung zu Kaspersky Security Network** wird geöffnet.

3. Lesen Sie die KSN-Erklärung und klicken Sie je nach Ihrer Entscheidung auf eine der folgenden Schaltflächen:

   - **Ich akzeptiere die aktualisierte KSN-Erklärung**
   - **Ich verwende KSN unter der alten Erklärung**

Entsprechend Ihrer Entscheidung funktioniert KSN in Übereinstimmung mit den Bedingungen der aktuellen oder der aktualisierten KSN-Erklärung. Das Anzeigen des Textes der akzeptierten KSN-Erklärung ist jederzeit in den Eigenschaften des Administrationsservers möglich.

Feststellen, ob der Verteilungspunkt als KSN-Proxyserver fungiert

Sie können auf einem verwalteten Gerät, welches als Verteilungspunkt fungiert, den KSN-Proxyserver aktiveren. Ein verwaltetes Gerät funktioniert als KSN-Proxyserver, wenn auf dem Gerät der Dienst "ksnproxy" ausgeführt wird. Sie können diesen Dienst lokal auf dem Gerät überprüfen, aktivieren und deaktivieren.

Sie können einem Windows-basierten oder Linux-basierten Gerät die Rolle des Verteilungspunkts zuweisen. Die Methode zur der Überprüfung des Verteilungspunkts hängt vom Betriebssystem dieses Verteilungspunkts ab.

So stellen Sie fest, ob der Windows-basierte Verteilungspunkt als KSN-Proxyserver fungiert:

1. Öffnen Sie auf dem Gerät mit dem Verteilungspunkt unter Windows die **Dienste**-App (**Alle Programme** → **Windows Verwaltungsprogramme** → **Dienste**).

2. Prüfen Sie in der Liste der Dienste, ob der Dienst ksnproxy ausgeführt wird.

   Wenn der Dienst "ksnproxy" ausgeführt wird, nimmt der Administrationsagent auf diesem Gerät an Kaspersky Security Network teil und fungiert als KSN-Proxyserver für verwaltete Geräte, die sich im Bereich des Verteilungspunkts befinden.

Bei Bedarf können Sie den Dienst ksnproxy deaktivieren. In diesem Fall nimmt der Administrationsagent des Verteilungspunkts nicht länger an Kaspersky Security Network teil. Dieser Vorgang erfordert lokale Administratorrechte.

So stellen Sie fest, ob der Linux-basierte Verteilungspunkt als KSN-Proxyserver fungiert:

1. Zeigen Sie auf dem Gerät, dass als Verteilungspunkt fungiert, die Liste der ausgeführten Prozesse an.

2. Überprüfen Sie, ob in der Liste der laufenden Prozesse, der Prozess `/[[/opt/kaspersky/ksc64/sbin/ksnproxy]]` ausgeführt wird.

Wenn der Dienst `/opt/kaspersky/ksc64/sbin/ksnproxy` ausgeführt wird, nimmt der Administrationsagent auf diesem Gerät an Kaspersky Security Network teil und fungiert als KSN-Proxyserver für verwaltete Geräte, die sich im Bereich des Verteilungspunkts befinden.

Szenario: Upgrades von Kaspersky Security Center und der verwalteten Sicherheitsanwendungen

Dieser Abschnitt bietet einen kurzen Überblick über das Hauptszenario des Upgrades von Kaspersky Security Center und der verwalteten Sicherheitsanwendungen.

Das Upgrade von Kaspersky Security Center und der verwalteten Sicherheitsanwendungen erfolgt in mehreren Schritten:

1. **Überprüfen der Hardware- und Softwarevoraussetzungen**

   Stellen Sie sicher, dass Ihre Hardware den Anforderungen entspricht, und installieren Sie sie die erforderlichen Updates.

2. **Planung der Ressourcen**

   Berechnen Sie, wie viel Speicherplatz Ihre Datenbank ungefähr belegt. Stellen Sie sicher, dass ausreichend Speicherplatz für die Backup-Kopie der Einstellungen des Administrationsservers und der Datenbank vorhanden ist.

3. **Installationsdatei für Kaspersky Security Center abrufen**

   Rufen Sie die ausführbare Datei der aktuellen Version von Kaspersky Security Center ab und speichern Sie diese auf dem Gerät, das als Administrationsserver fungieren soll. Lesen Sie sich die Versionshinweise zu der Version von Kaspersky Security Center durch, die Sie verwenden möchten.

4. **Backup-Kopie der Vorgängerversion erstellen**

   Erstellen Sie mithilfe des Tools zum Anlegen und Wiederherstellen eines Daten-Backups eine Backup-Kopie der Administrationsserverdaten. Sie können außerdem eine Aufgabe zum Anlegen eines Backups erstellen.

   Es wird empfohlen, die Liste der installierten Plug-ins zu exportieren.

5. **Installer ausführen**

   Starten Sie die ausführbare Datei der aktuellen Version von Kaspersky Security Center. Geben Sie beim Start dieser Datei an, dass Sie eine Backup-Kopie besitzen, und geben Sie ihren Speicherort an. Ihre Daten werden aus dem Backup wiederhergestellt.

6. **Upgrade der verwalteten Programme**

   Wenn eine neuere Version des Programms vorliegt, können Sie ein Upgrade vornehmen. Lesen Sie die Liste der unterstützten Kaspersky-Anwendungen und stellen Sie sicher, dass Ihre Version von Kaspersky Security Center mit dieser Anwendung kompatibel ist. Nehmen Sie anschließend das Upgrade des Programms unter Beachtung der Versionshinweise vor.

Ergebnisse

Stellen Sie nach Abschluss des Upgrade-Szenarios sicher, dass die neue Version des Administrationsservers erfolgreich in der Microsoft Management Console installiert wurde. Klicken Sie auf **Hilfe → Über Kaspersky Security Center**. Die Version wird angezeigt.

Um sicherzustellen, dass Sie die neue Version des Administrationsservers in der Kaspersky Security Center Web Console verwenden, klicken Sie im oberen Bereich des Bildschirms auf das Symbol Einstellungen ( ) neben dem Namen des Administrationsservers. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers auf der Registerkarte **Allgemein** den Abschnitt **Allgemein**. Die Version wird angezeigt.

Wenn Sie die Daten des Administrationsservers wiederherstellen müssen, befolgen Sie die im folgenden Artikel beschriebenen Schritte: Anlegen und Wiederherstellen eines Daten-Backups im interaktiven Modus.

Wenn Sie eine verwaltete Sicherheitsanwendung aktualisiert haben, stellen Sie sicher, dass sie auf dem verwalteten Gerät ordnungsgemäß installiert wurde. Weitere Informationen finden Sie in der Dokumentation zu diesem Programm.

Datenbanken und Programme von Kaspersky aktualisieren

Dieser Abschnitt beschreibt die Schritte, die Sie für ein regelmäßiges Update durchführen müssen:

- Kaspersky-Datenbanken und Programm-Module
- Installierte Kaspersky-Anwendungen, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Szenario: Datenbanken und Programme von Kaspersky regelmäßig aktualisieren

Dieser Abschnitt enthält ein Szenario zum regelmäßigen Update der Datenbanken, Softwaremodule und Anwendungen von Kaspersky. Nachdem Sie das Szenario "Netzwerkschutz konfigurieren" abgeschlossen haben, müssen Sie die Verlässlichkeit des Schutzsystems aufrecht erhalten, um sicherzustellen, dass die Administrationsserver und die verwalteten Geräte dauerhaft gegen verschiedene Bedrohungen wie Viren, Netzwerkangriffe und Phishing-Attacken geschützt sind.

Der Netzwerkschutz bleibt auf dem neuesten Stand, wenn folgende Komponenten regelmäßig aktualisiert werden:

- Kaspersky-Datenbanken und Programm-Module
- Installierte Kaspersky-Anwendungen, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen

Wenn Sie dieses Szenario abschließen, können Sie sicher sein, dass:

- Ihr Netzwerk durch die aktuellsten Programme von Kaspersky, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen, geschützt ist.
- die Antiviren-Datenbanken und andere, für die Sicherheit des Netzwerks kritische Kaspersky-Datenbanken, immer auf dem neuesten Stand sind.

Erforderliche Vorrausetzungen

Die verwalteten Geräte benötigen eine Verbindung zum Administrationsserver. Wenn sie keine Verbindung haben, erwägen Sie eine manuelle Aktualisierung der Datenbanken von Kaspersky, Programm-Module und Programme oder eine Aktualisierung direkt von den Kaspersky-Update-Servern.

Der Administrationsserver muss eine Verbindung zum Internet haben.

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

1. die Sicherheitsanwendungen von Kaspersky gemäß dem Szenario zur Verteilung von Kaspersky-Anwendungen via Kaspersky Security Center Web Console auf den verwalteten Geräten verteilt haben.
2. alle notwendigen Richtlinien, Richtlinienprofile und Aufgaben entsprechend dem Szenario "Konfiguration des Netzwerkschutzes" konfiguriert haben.
3. in Übereinstimmung mit der Anzahl der verwalteten Geräte und der Netzwerktopologie eine geeignete Anzahl an Verteilungspunkten zugewiesen haben.

Das Update der Datenbanken und Anwendungen von Kaspersky erfolgt in mehreren Schritten:

1. **Auswählen eines Update-Schemas**

   Es existieren verschiedene Schemas die Sie nutzen können, um Updates für die Komponenten des Kaspersky Security Centers und Sicherheitsanwendungen zu installieren. Wählen Sie ein Schema oder mehrere Schemas, welche die Anforderungen Ihres Netzwerks am besten erfüllen.

2. **Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen**

   Diese Aufgabe wird automatisch vom Schnellstartassistent des Kaspersky Security Centers erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe jetzt.

   Diese Aufgabe wird benötigt, um Updates von den Kaspersky-Update-Servern in die Datenverwaltung des Administrationsservers zu laden, und um die Updates der Kaspersky-Datenbanken und Programm-Module des Kaspersky Security Centers auszuführen. Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, werden die Updates aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte geladen. In diesem Fall laden die verwalteten Geräte, die sich im Bereich eines Verteilungspunktes befinden, die Updates aus der Datenverwaltung des Verteilungspunktes, anstatt aus der Datenverwaltung des Administrationsservers.

   Anleitung:

   - Verwaltungskonsole: Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen
   - Kaspersky Security Center Web Console: Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen

3. **Aufgabe zum Download von Updates in die Datenverwaltung auf Verteilungspunkte erstellen (optional)**

   Standardmäßig werden die Updates von den Verteilungspunkten vom Administrationsserver heruntergeladen. Sie können Kaspersky Security Center so konfigurieren, dass die Verteilungspunkte die Updates direkt von den Kaspersky-Update-Servern herunterladen. Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt und die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* erstellt wurde, laden die Verteilungspunkte Updates von den Kaspersky-Update-Servern herunter, und nicht von der Datenverwaltung des Administrationsservers.

   Anleitung:

   - Verwaltungskonsole: Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen
   - Kaspersky Security Center Web Console: Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

4. **Konfigurieren der Verteilungspunkte**

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, stellen Sie sicher, dass die Option **Updates verteilen** in den Einstellungen aller benötigten Verteilungspunkten aktiviert ist. Wenn diese Option für einen Verteilungspunkt deaktiviert ist, laden die Geräte, die sich im Bereich dieses Verteilungspunktes befinden, die Updates von der Datenverwaltung des Administrationsservers herunter.

   Wenn Sie möchten, dass verwaltete Geräte ihre Updates nur über Verteilungspunkte erhalten, aktivieren Sie die Option **Dateien nur über Verteilungspunkte übertragen** in der Richtlinie des Administrationsagenten.

5. **Optimieren des Update-Vorgangs durch die Nutzung des autonomen Modells für den Update-Download oder mithilfe von Diff-Dateien (optional)**

   Sie können den Prozesses durch die Nutzung des autonomen Modells für den Download von Updates (standardmäßig aktiviert) oder durch die Nutzung von Diff-Dateien optimieren. Für jedes Netzwerksegment müssen Sie eine der beiden Funktionen auswählen, da diese nicht simultan arbeiten können.

   Wenn das autonome Modell für den Download von Updates aktiviert ist, lädt der Administrationsagent die benötigten Updates auf das verwaltete Gerät. Dies geschieht, sobald die Updates in die Datenverwaltung des Administrationsservers geladen wurden und bevor die Sicherheitsanwendung die Updates anfragt. Dies erhöht die Verlässlichkeit des Update-Prozesses. Um diese Funktion zu nutzen, aktivieren Sie die Option **Updates und Antiviren-Datenbanken im Voraus vom Administrationsserver herunterladen (empfohlen)** in der Richtlinie des Administrationsagenten.

   Wenn Sie das autonome Modell für den Download von Updates nicht benutzen, können Sie den Datenverkehr zwischen Administrationsserver und verwalteten Geräten optimieren, indem Sie Diff-Dateien benutzen. Wenn diese Funktion aktiviert ist, laden der Administrationsserver oder ein Verteilungspunkt im Gegensatz zu ganzen Kaspersky-Datenbank-Dateien oder Programm-Modulen nur Diff-Dateien herunter. Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Deswegen benötigt eine Diff-Datei weniger Platz als eine ganze Datei. Dies resultiert in einem verringerten Datenverkehr zwischen dem Administrationsserver oder Verteilungspunkt und den verwalteten Geräten. Um diese Funktion zu nutzen, aktivieren Sie die Option **Diff-Dateien herunterladen** in den Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und/oder der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*.

   Anleitung:

   - Diff-Dateien zum Update von Kaspersky-Datenbanken und -Software-Modulen verwenden
   - Verwaltungskonsole: Autonomes Modell für den Download von Updates aktivieren und deaktivieren
   - Kaspersky Security Center Web Console: Autonomes Modell für den Download von Updates aktivieren und deaktivieren

6. **Heruntergeladene Updates prüfen (optional)**

   Bevor Sie heruntergeladene Updates installieren, können Sie diese mit der Aufgabe zur *Update-Prüfung* überprüfen. Diese Aufgabe führt die anhand von Einstellungen für die angegebene Sammlung von Testgeräten konfigurierten Aufgaben zum Geräte-Update und zur Schadsoftware-Untersuchung nacheinander aus. Nach Erhalt des Resultats der Aufgabe, startet oder blockiert der Administrationsserver die Verteilung der Updates auf die verbliebenen Geräte.

   Die Aufgabe zur *Update-Prüfung* kann im Rahmen der Aufgabe für den *Download von Updates in die Datenverwaltung des Administrationsservers* ausgeführt werden. Aktivieren Sie in der Verwaltungskonsole in den Einstellungen der Aufgabe zum *Download von Updates in die Datenverwaltung des Administrationsservers* die Option **Update-Prüfung vor der Verteilung ausführen** oder in der Kaspersky Security Center Web Console die Option **Update-Prüfung ausführen**.

   Anleitung:

   - Verwaltungskonsole: Heruntergeladene Updates prüfen
   - Kaspersky Security Center Web Console: Heruntergeladene Updates prüfen

7. **Genehmigen und Ablehnen von Software-Updates**

   Standardmäßig besitzen heruntergeladene Software-Updates den Status *Nicht definiert*. Sie können den Status auf *Genehmigt* oder *Abgelehnt* ändern. Genehmigte Updates werden immer installiert. Wenn ein Update eine Überprüfung und ein Akzeptieren des Endbenutzer-Lizenzvertrags benötigt, müssen Sie die Bestimmungen zuerst akzeptieren. Danach kann das Update an die verwalteten Geräte verteilt werden. Die nicht definierten Updates können nur in Übereinstimmungen mit den Richtlinieneinstellungen des Administrationsagenten auf dem Administrationsagent und auf anderen Komponenten von Kaspersky Security Center installiert werden. Updates, für die Sie den Status *Abgelehnt* gewählt haben, werden auf den Geräten nicht installiert. Wenn ein abgelehntes Update für eine Sicherheitsanwendung bereits zuvor installiert wurde, wird Kaspersky Security Center versuchen, dieses Update von allen Geräten zu deinstallieren.

   Das Genehmigen und Ablehnen von Updates ist nur für Administrationsagenten und verwaltete Kaspersky-Anwendungen verfügbar, die auf Windows- oder Linux-basierten Client-Geräten installiert sind. Eine nahtlose Aktualisierung wird von den folgenden Komponenten nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung.

   Anleitung:

   - Verwaltungskonsole: Genehmigen und Ablehnen von Programm-Updates
   - Kaspersky Security Center Web Console: Genehmigen und Ablehnen von Programm-Updates

8. **Konfiguration der automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center**

   Die heruntergeladenen Updates und Patches für den Administrationsagenten und andere Komponenten von Kaspersky Security Center werden automatisch installiert. Wenn Sie die Option **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren** in den Einstellungen des Administrationsagenten aktiviert haben, werden alle Updates nach dem Herunterladen in die Datenverwaltung (oder in mehrere Datenverwaltungen) automatisch installiert. Wenn die Option deaktiviert ist, werden die Patches von Kaspersky, die heruntergeladen und mit dem Status *Nicht festgestellt* markiert sind, erst installiert, wenn Sie ihren Status auf *Genehmigt* ändern.

   Anleitung:

   - Verwaltungskonsole: Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren
   - Kaspersky Security Center Web Console: Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren

9. **Installation von Updates für den Administrationsserver**

   Programm-Updates für den Administrationsserver sind nicht vom Update-Status abhängig. Sie werden nicht automatisch installiert und müssen zunächst durch den Administrator auf der Registerkarte **Überwachung** in der Verwaltungskonsole (**Administrationsserver** `<Servername>` → **Überwachung**), oder in dem Abschnitt **Benachrichtigungen** in der Kaspersky Security Center Web Console (**Überwachung und Berichterstattung** → **Benachrichtigungen**) genehmigt werden. Danach muss der Administrator die Installation der Updates explizit ausführen.

10. **Konfiguration der automatischen Installation von Updates für die Sicherheitsanwendungen**

    Erstellen Sie die Aufgabe *Update* für verwaltete Programme, um zeitnahe Updates für die Anwendungen, Programm-Module und Kaspersky-Datenbanken (einschließlich der Antiviren-Datenbanken) zu gewährleisten. Um zeitnahe Updates zu gewährleisten, wird es empfohlen, dass Sie beim Konfigurieren des Aufgabenzeitplans die Option **Nach dem Download von Updates in die Datenverwaltung** auswählen.

    Wenn Ihr Netzwerk ausschließlich IPv6-Geräte enthält und Sie regelmäßig die auf den Geräten installierten Sicherheitsanwendungen aktualisieren wollen, stellen Sie sicher, das auf den verwalteten Geräten jeweils der Administrationsserver und der Administrationsagent ab der Version 13.2 installiert sind.

Standardmäßig werden Updates für Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Security für Linux erst installiert, nachdem der Update-Status auf *Genehmigt* geändert wurde. Sie können die Update-Einstellungen in der Aufgabe *Update* ändern.

Wenn ein Update eine Überprüfung und ein Akzeptieren des Endbenutzer-Lizenzvertrags benötigt, müssen Sie die Bestimmungen zuerst akzeptieren. Danach kann das Update an die verwalteten Geräte verteilt werden.

Anleitung:

- Verwaltungskonsole: Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren
- Kaspersky Security Center Web Console: Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren

Ergebnisse

Bei Abschluss des Szenarios ist Kaspersky Security Center so konfiguriert, dass die Updates der Kaspersky-Datenbanken und installierten Kaspersky-Anwendungen ausgeführt werden, nachdem die Updates in die Datenverwaltung des Administrationsservers oder der Verteilungspunkte geladen werden. Anschließend können Sie mit der Überwachung des Netzwerkstatus fortfahren.

Über das Aktualisieren der Datenbanken, Software-Module und Programme von Kaspersky

Um sicherzustellen, dass der Schutz Ihrer Administrationsserver und verwalteten Geräte auf dem neuesten Stand ist, müssen Sie zeitnah Updates bereitstellen für:

- Kaspersky-Datenbanken und Programm-Module

  Vor dem Herunterladen von Kaspersky-Datenbanken und Softwaremodulen überprüft Kaspersky Security Center, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Dies ist erforderlich, um sicherzustellen, dass die Antiviren-Datenbanken aktualisiert werden und das Sicherheitsniveau für die verwalteten Geräte beibehalten wird.

- Installierte Kaspersky-Anwendungen, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen

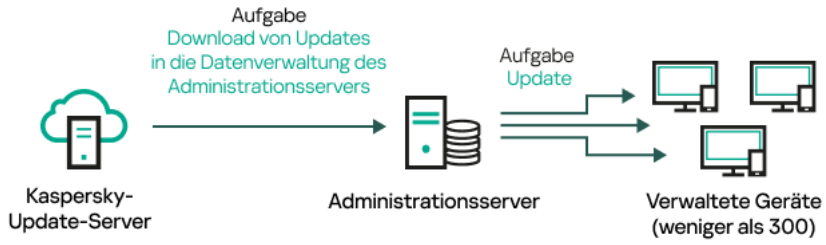
  Kaspersky Security Center ermöglicht Ihnen die automatische Aktualisierung des Administrationsagenten und der Kaspersky-Anwendungen auf Geräten mit Windows und Linux. Ein nahtloses Update der folgenden Komponenten wird nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung. Um diese Komponenten zu aktualisieren, müssen Sie die jeweils aktuellste Version von der Kaspersky-Website herunterladen und anschließend manuell installieren.

Abhängig von der Konfiguration Ihres Netzwerks können Sie die folgenden Schemata für das Herunterladen und Verteilen der erforderlichen Updates auf die verwalteten Geräte verwenden:

- Durch Verwendung einer einzelnen Aufgabe: *Download von Updates in die Datenverwaltung des Administrationsservers*
- Durch Verwendung zweier Aufgaben:
  - Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*
  - Die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*
- Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server
- Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security auf den verwalteten Geräten
- Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Verwenden der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers

In diesem Schema lädt Kaspersky Security Center über die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* Updates herunter. In kleinen Netzwerken, die weniger als 300 verwaltete Geräte in einem einzelnen Netzwerksegment oder weniger als 10 verwaltete Geräte in jedem Netzwerksegment enthalten, werden die Updates direkt aus der Datenverwaltung des Administrationsservers auf die verwalteten Geräte verteilt (siehe Abbildung unten).

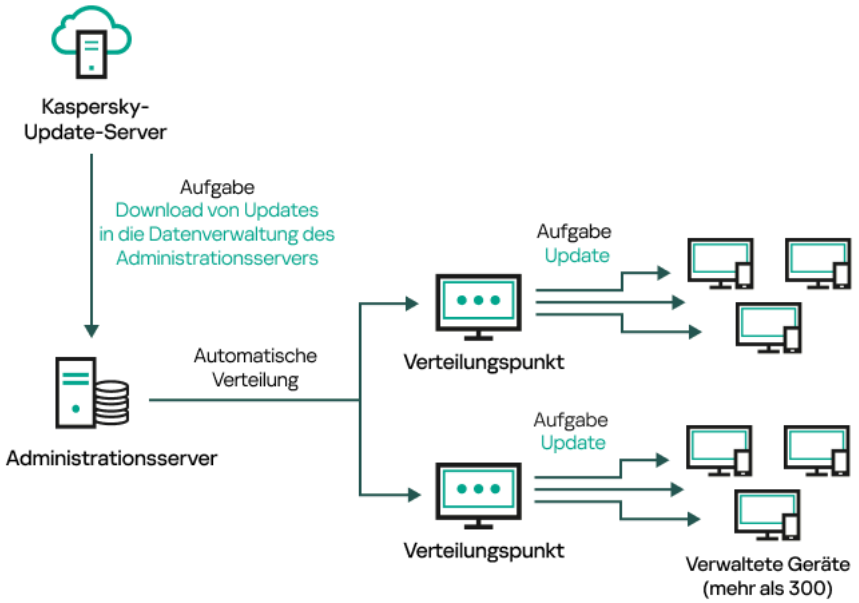


Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers ohne Verteilungspunkte

Standardmäßig verwendet der Administrationsserver zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können Administrationsserver so einrichten, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Wenn Ihr Netzwerk mehr als 300 verwaltete Geräte in einem einzigen Netzwerksegment enthält oder wenn Ihr Netzwerk aus mehreren Netzwerksegmenten mit mehr als 9 verwalteten Geräten in jedem Netzwerksegment besteht, empfehlen wir Ihnen, Verteilungspunkte zu verwenden, um die Updates auf die verwalteten Geräte zu übertragen (siehe Abbildung unten). Verteilungspunkte reduzieren die Belastung des Administrationsservers und optimieren den Datenverkehr zwischen dem Administrationsserver und den verwalteten Geräten. Sie können die Anzahl und Konfiguration der für Ihr Netzwerk benötigten Verteilungspunkte berechnen.

In diesem Schema werden die Updates automatisch aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte heruntergeladen. Die verwalteten Geräte, die zum Umfang eines Verteilungspunkts gehören, laden die Updates aus der Datenverwaltung des Verteilungspunkts anstelle der Datenverwaltung des Administrationsservers herunter.



Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers mit Verteilungspunkten

Wenn die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* abgeschlossen ist, werden die folgenden Updates in die Datenverwaltung des Administrationsservers heruntergeladen:

- Kaspersky-Datenbanken und Softwaremodule für Kaspersky Security Center

  Diese Updates werden automatisch installiert.

- Kaspersky-Datenbanken und Softwaremodule für die Sicherheitsanwendungen auf den verwalteten Geräten

  Diese Updates werden durch die Update-Aufgabe für Kaspersky Endpoint Security für Windows installiert.

- Updates für den Administrationsserver

  Diese Updates werden nicht automatisch installiert. Der Administrator muss die Installation der Updates ausdrücklich genehmigen und durchführen.

  > Für die Ins von Patches auf dem Administrationsserver sind lokale Administratorrechte erforderlich.

- Updates für die Komponenten von Kaspersky Security Center

  Standardmäßig werden diese Updates automatisch installiert. Sie können die Einstellungen in den Administrationsagent-Richtlinien ändern.

- Updates für die Sicherheitsanwendungen

  Standardmäßig installiert Kaspersky Endpoint Security für Windows nur die Updates, die Sie genehmigen (Die Updates können Sie über die Verwaltungskonsole oder über Kaspersky Security Center Web Console genehmigen). Die Updates werden mit der Aufgabe *Update* installiert und können in den Eigenschaften dieser Aufgabe konfiguriert werden.

Die Aufgabe zum *Download von Updates in die Datenverwaltung des Administrationsservers* steht auf virtuellen Administrationsservern nicht zur Verfügung. In der Datenverwaltung des virtuellen Administrationsservers werden Updates angezeigt, die auf den primären Administrationsserver heruntergeladen wurden.

Sie können die Updates, die auf Funktionsfähigkeit und Fehler geprüft werden sollen, auf einer Reihe von Testgeräten konfigurieren. Wenn die Überprüfung erfolgreich ist, werden die Updates an andere verwaltete Geräte verteilt.

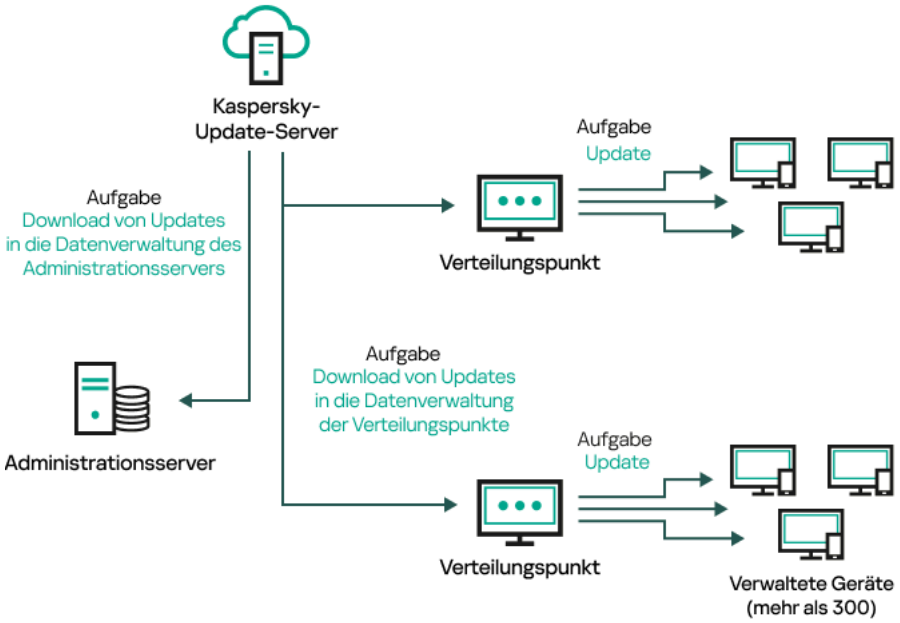
Jede Anwendung von Kaspersky fordert die erforderlichen Updates vom Administrationsserver an. Der Administrationsserver aggregiert diese Anforderungen und lädt nur die Aktualisierungen herunter, die von einer Anwendung angefordert werden. Dadurch wird sichergestellt, dass die gleichen Updates nicht mehrmals heruntergeladen werden und unnötige Updates überhaupt nicht heruntergeladen werden. Bei der Ausführung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* der Administrationsserver die folgenden Informationen automatisch an Kaspersky-Update-Server, um das Herunterladen von relevanten Versionen der Kaspersky-Datenbanken und Programm-Module sicherzustellen:

- Anwendungs-ID und Version des Programms
- ID der Programminstallation
- ID des aktiven Schlüssels
- Ausführungs-ID der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*

Keine der übermittelten Informationen enthält persönliche oder andere vertrauliche Daten. AO Kaspersky Lab schützt die erhaltenen Informationen in Übereinstimmung mit den geltenden gesetzlich festgelegten Anforderungen.

Verwendung von zwei Aufgaben: Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers und Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

Sie können Updates für die Datenverwaltungen der Verteilungspunkte direkt von den Update-Servern von Kaspersky anstelle der Datenverwaltung des Administrationsservers herunterladen und die Updates dann auf die verwalteten Geräte verteilen (siehe Abbildung unten). Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.



Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers und der Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

Standardmäßig verwenden der Administrationsserver und die Verteilungspunkte zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können den Administrationsserver und/oder die Verteilungspunkte so konfigurieren, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Um dieses Schema zu implementieren, erstellen Sie die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* zusätzlich zur Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*. Danach laden die Verteilungspunkte die Updates von den Kaspersky Update-Servern herunter und nicht von der Datenverwaltung des Administrationsservers.

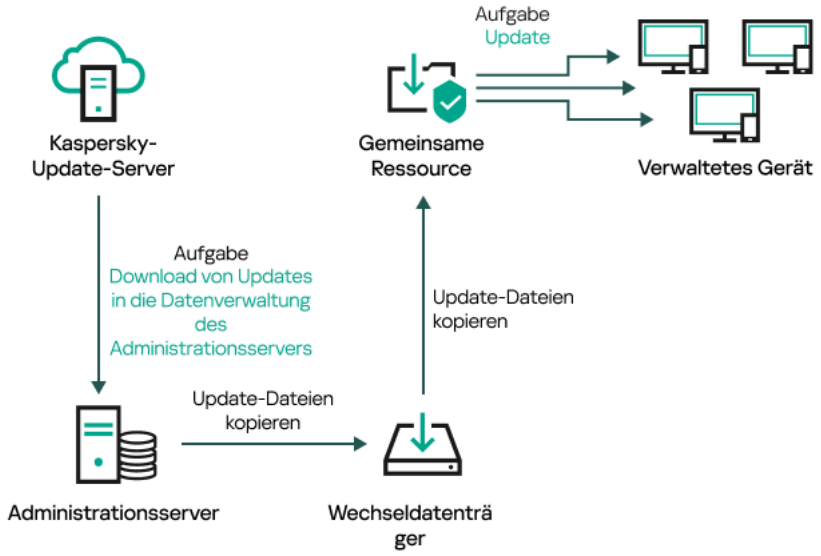
Geräte mit Verteilungspunkten unter macOS können keine Updates von Kaspersky Update-Servern herunterladen.

Wenn ein oder mehrere Geräte, die unter macOS laufen, in den Bereich der Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* fallen, schließt die Aufgabe mit dem Status *Fehlgeschlagen* ab, selbst wenn sie auf allen Windows-Geräten erfolgreich abgeschlossen wurde.

Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* wird auch für dieses Schema benötigt, da mit dieser Aufgabe Datenbanken und Softwaremodule von Kaspersky für das Kaspersky Security Center heruntergeladen werden können.

Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Wenn die Client-Geräte keine Verbindung zum Administrationsserver haben, können Sie einen lokalen Ordner oder eine freigegebene Ressource als Quelle für das Update von Kaspersky-Datenbanken, -Softwaremodulen und -Anwendungen verwenden. In diesem Schema müssen Sie die erforderlichen Updates aus der Datenverwaltung des Administrationsservers auf einen Wechseldatenträger und dann in den lokalen Ordner oder die als Update-Quelle in den Einstellungen von Kaspersky Endpoint Security angegebene freigegebene Ressource kopieren (siehe Abbildung unten).



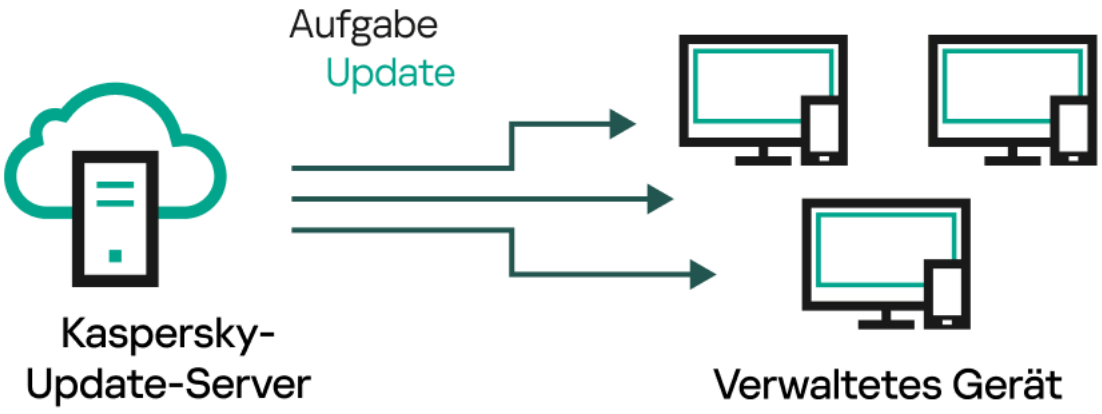
Manuelles Upgrade über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Weitere Informationen zu Update-Quellen in Kaspersky Endpoint Security finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux

Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security auf den verwalteten Geräten

Auf den verwalteten Geräten können Sie Kaspersky Endpoint Security so konfigurieren, dass Updates direkt von den Updateservern von Kaspersky empfangen werden (siehe Abbildung unten).



Updates von Sicherheitsanwendungen direkt von Kaspersky Update-Servern aus

In diesem Schema verwendet die Sicherheitsanwendung nicht die vom Kaspersky Security Center bereitgestellten Datenverwaltungen. Um Updates direkt von den Update-Servern von Kaspersky zu erhalten, geben Sie in der Schnittstelle der Sicherheitsanwendung die Update-Server von Kaspersky als Update-Quelle an. Weitere Informationen zu diesen Einstellungen finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux

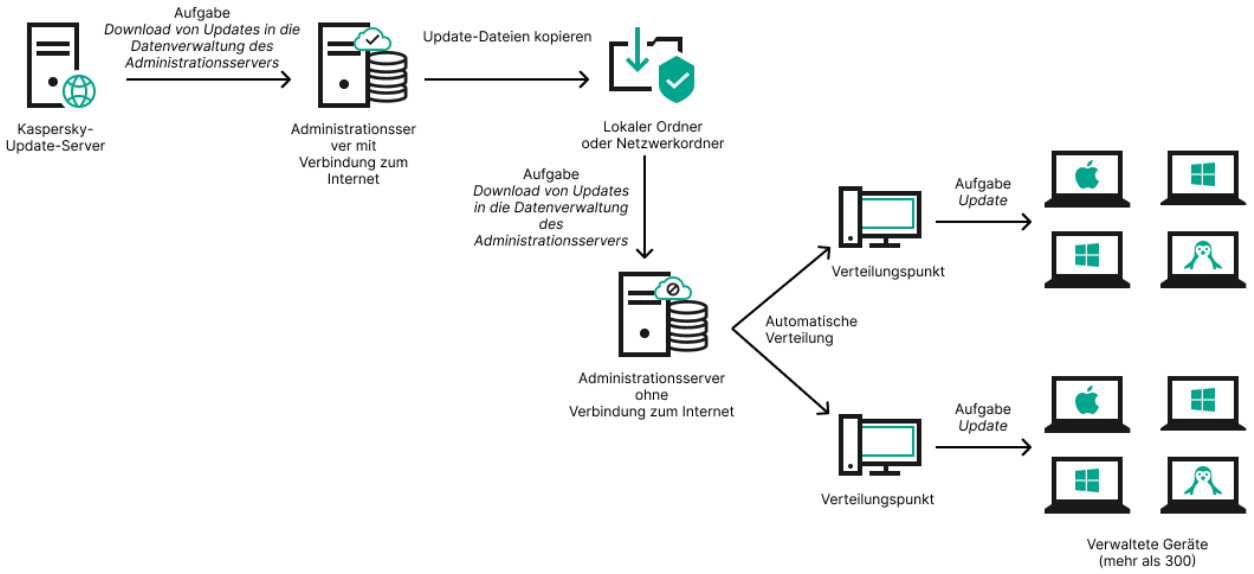
Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Wenn der Administrationsserver keine Internetverbindung hat, können Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zum Herunterladen von Updates aus einem lokalen oder Netzwerkordner konfigurieren. In diesem Fall müssen Sie die erforderlichen Update-Dateien von Zeit zu Zeit in den angegebenen Ordner kopieren. Beispielsweise können Sie die erforderlichen Update-Dateien aus einer der folgenden Quellen kopieren:

- Administrationsserver mit Internetverbindung (siehe Abbildung unten)

  Da ein Administrationsserver nur die Updates herunterlädt, die von den Sicherheitsanwendungen angefordert werden, müssen die Gruppen der Sicherheitsanwendungen, die von den Administrationsservern verwaltetet werden – d. h. von dem mit Internetverbindung und dem ohne Internetverbindung – übereinstimmen.

  Wenn der von Ihnen zum Herunterladen von Updates verwendete Administrationsserver die Version 13.2 besitzt, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option **Updates nach altem Schema herunterladen**.



Aktualisieren mittels eines lokalen Ordners oder Netzwerkordners, wenn der Administrationsserver keine Internetverbindung hat

- Kaspersky Update Utility

  Da dieses Tool das alte Schema zum Herunterladen von Updates verwendet, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option **Updates nach altem Schema herunterladen**.

Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen

Die Administrationsserver-Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* wird automatisch durch den Schnellstartassistenten von Kaspersky Security Center erstellt. Sie können nur eine Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* erstellen. Deshalb können Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* nur dann erstellen, wenn sie aus der Liste mit Aufgaben des Administrationsservers entfernt wurde.

Diese Aufgabe ist erforderlich, um Updates von Kaspersky-Update-Servern in die Datenverwaltung des Administrationsservers herunterzuladen. Die Liste der Updates enthält:

- Updates von Datenbanken und Softwaremodulen für den Administrationsserver
- Updates von Datenbanken und Softwaremodulen für Kaspersky-Sicherheitsanwendungen
- Updates der Kaspersky Security Centers-Komponenten
- Updates von Kaspersky-Sicherheitsanwendungen

Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

Bevor Sie Updates an die verwalteten Geräte verteilen, können Sie die Aufgabe zur *Update-Prüfung* ausführen. Dadurch können Sie sicherstellen, dass der Administrationsserver die heruntergeladenen Updates ordnungsgemäß installiert und die Sicherheitsstufe durch die Updates nicht verringert wird. Um sie vor dem Verteilen zu überprüfen, konfigurieren Sie die Option **Update-Prüfung ausführen** in den Einstellungen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

*So erstellen Sie die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers**:*

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Download von Updates in die Datenverwaltung des Administrationsservers**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.
6. Klicken Sie auf **Erstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste angezeigt.
7. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
8. Geben Sie im Fenster mit den Aufgabeneigenschaften auf der Registerkarte **Programmeinstellungen** die folgenden Einstellungen an:

   - **Update-Quellen**

     Als Update-Quelle für den Administrationsserver können die folgenden Ressourcen verwendet werden:

     - Kaspersky-Update-Server

HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen. Standardmäßig verwendet der Administrationsserver zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können Administrationsserver so einrichten, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Standardmäßig ausgewählt.

- Primärer Administrationsserver

  Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.

- Lokaler Ordner oder Netzwerkordner

  Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Ein Netzwerkordner kann ein FTP- oder HTTP-Server oder eine SMB-Freigabe sein. Für Netzwerkordner, die eine Authentifizierung erfordern, wird nur das SMB-Protokoll unterstützt. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

  > Ein FTP- oder HTTP-Server oder ein Netzwerkordner, der von einer Update-Quelle verwendet wird, muss eine Ordnerstruktur (mit Updates) enthalten, die der Struktur entspricht, die bei Verwendung der Kaspersky-Update-Server erstellt wurde.

Falls ein freigegebener Ordner mit Updates passwortgeschützt ist, aktivieren Sie die Option **Benutzerkonto für den Zugriff auf den freigegebenen Ordner der Update-Quelle angeben (falls vorhanden)** und geben Sie die für den Zugriff erforderlichen Anmeldeinformationen ein.

- **Ordner zum Speichern von Updates**

  Der Pfad zum angegebenen Ordner, in dem die bezogenen Updates gespeichert werden. Sie können den Pfad des angegebenen Ordners in die Zwischenablage kopieren. Für eine Gruppenaufgabe können Sie den Pfad eines angegebenen Ordners nicht ändern.

- Sonstige Einstellungen:

  - **Update der sekundären Administrationsserver erzwingen**

    Wenn diese Option aktiviert ist, startet der Administrationsserver die Update-Aufgaben auf den sekundären Administrationsservern sobald neue Updates heruntergeladen werden. Update-Aufgaben werden unter Verwendung der Update-Quellen gestartet, die in den Aufgabeneigenschaften auf den sekundären Administrationsservern konfiguriert ist.

    Wenn diese Option deaktiviert ist, werden die Update-Aufgaben auf den sekundären Administrationsservern gemäß ihren Zeitplänen gestartet.

    Diese Option ist standardmäßig deaktiviert.

  - **Heruntergeladene Updates in zusätzliche Ordner kopieren**

    Nachdem der Administrationsserver Updates empfängt, kopiert er sie in die angegebenen Ordner. Verwenden Sie diese Option, wenn Sie die Verteilung von Updates in Ihrem Netzwerk manuell verwalten möchten.

Sie können diese Option beispielsweise in der folgenden Situation verwenden: Das Netzwerk Ihres Unternehmens besteht aus mehreren unabhängigen Subnetzen, wobei Geräte in den einzelnen Subnetzen über keinen Zugriff auf andere Subnetze verfügen. Allerdings haben Geräte in allen Teilnetzen Zugriff auf eine gemeinsame Netzwerkfreigabe. In diesem Fall müssen Sie den Administrationsserver in einem der Subnetze einrichten, um Updates von den Kaspersky-Update-Servern herunterzuladen. Aktivieren Sie diese Option und geben Sie dann diese Netzwerkfreigabe an. Geben Sie bei heruntergeladenen Updates der Repository-Aufgaben für andere Administrationsserver die gleiche Netzwerkfreigabe wie für die Update-Quelle an.

Wenn Sie auswählen, dass die Updates in einen lokalen Ordner kopiert werden sollen, müssen Sie einen Ordner auf dem Gerät mit dem installierten Administrationsserver angeben. Der Pfad des Ordners hängt vom Betriebssystem auf dem Gerät ab. Da sich der lokale Ordner auf einem Linux-basierten Administrationsserver befindet, müssen Sie den POSIX-Pfad angeben. Beispiel: /Pfad/zum/Verzeichnis.

Wenn Sie einen Netzwerkordner auswählen, der sich auf einem Linux-Administrationsserver befindet, müssen Sie vorher durch das Mounten des Ordners sicherstellen, dass von dem Gerät mit installiertem Administrationsserver auf den Netzwerkordner zugegriffen werden kann. Der Zugriff auf den Ordner erfolgt über das SMB-Protokoll.

Diese Option ist standardmäßig deaktiviert.

- **Update der Geräte und sekundären Administrationsserver bis Abschluss des Kopierens nicht erzwingen**

  Die Aufgaben zum Herunterladen von Updates auf Client-Geräte und sekundäre Administrationsserver werden erst gestartet, nachdem diese Updates vom Update-Hauptordner in die zusätzlichen Ordner kopiert wurden.

  Diese Option muss aktiviert sein, wenn Client-Geräte und sekundäre Administrationsserver Updates von zusätzlichen Netzwerkordnern herunterladen.

  Diese Option ist standardmäßig deaktiviert.

- **Inhalt der Updates**:

  - **Diff-Dateien herunterladen**

    Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

    Diese Option ist standardmäßig deaktiviert.

- **Updates nach altem Schema herunterladen**

  Ab Version 14 lädt Kaspersky Security Center die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit die Anwendung die Updates mithilfe des neuen Schemas herunterladen kann, muss die Update-Quelle die Update-Dateien mit den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Update-Quelle die Update-Dateien mit Metadaten enthält, die nur mit dem alten Schema kompatibel sind, aktivieren Sie die Option **Updates nach altem Schema herunterladen**. Andernfalls schlägt die Aufgabe zum Update-Download fehl.

  Sie müssen diese Option beispielsweise aktivieren, wenn als Update-Quelle ein lokaler Ordner oder ein Netzwerkordner angegeben sind, und wenn die Updatedateien in diesem Ordner von einer der folgenden Anwendungen heruntergeladen wurden:

  - Kaspersky Update Utility

    Dieses Tool lädt Updates unter Verwendung des alten Schemas herunter.

- Kaspersky Security Center 13.2 oder frühere Version

  Beispiel: Ihr Administrationsserver 1 besitzt keine Internetverbindung. In diesem Fall können Sie Updates über einen 2. Administrationsserver herunterladen, welcher über eine Internetverbindung verfügt, und welcher die Updates anschließend in einem lokalen Ordner oder Netzwerkordner ablegt. Dieser dient wiederum als Update-Quelle für den 1. Administrationsserver. Wenn der Administrationsserver 2 mit Version 13.2 oder früher läuft, aktivieren Sie die Option **Updates nach altem Schema herunterladen** in der Aufgabe für Administrationsserver 1.

Diese Option ist standardmäßig deaktiviert.

- **Update-Prüfung ausführen**

  Der Administrationsserver lädt Updates von der Quelle herunter, speichert sie in einer temporären Datenverwaltung und führt die Aufgabe aus, die im Feld **Aufgabe zur Update-Prüfung** angegeben wurde. Wenn die Aufgabe erfolgreich beendet wird, werden die Updates von der temporären Datenverwaltung in einen freigegebenen Ordner auf dem Administrationsserver kopiert und anschließend auf alle Geräte verteilt, für die der Administrationsserver als Update-Quelle dient (Aufgaben mit dem Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** werden gestartet). Die Aufgabe zum Download von Updates in die Datenverwaltung wird erst nach Abschluss der Aufgabe zur *Update-Prüfung* beendet.

  Diese Option ist standardmäßig deaktiviert.

9. Erstellen Sie im Fenster mit den Aufgabeneigenschaften auf der Registerkarte **Zeitplan** einen Zeitplan für den Aufgabenstart. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **Aufgabe starten**

     Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

     - **Manuell**

       Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

       Diese Variante ist standardmäßig ausgewählt.

     - **Alle n Minuten**

       Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

       Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

     - **Alle n Stunden**

       Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

       Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

     - **Alle n Tage**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

       Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

- Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
- Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

  Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
- Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

- **Aufgabe unterbrechen, wenn deren Ausführung länger dauert als**

  Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

10. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.

Nach Fertigstellung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* werden die Datenbanken-Updates und Updates der Programm-Module von der Update-Quelle geladen und im freigegebenen Ordner des Administrationsservers gespeichert. Wenn die Aufgabe für eine Administrationsgruppe erstellt wird, kommt sie nur auf Administrationsagenten zur Anwendung, die zur angegebenen Administrationsgruppe gehören.

Updates werden aus dem gemeinsamen Ordner des Administrationsservers an Client-Geräte und sekundäre Administrationsserver verteilt.

Heruntergeladene Updates prüfen

Bevor Sie Updates auf den verwalteten Geräten installieren, können Sie die Updates zunächst über die Aufgabe zur *Update-Prüfung* auf Funktionsfähigkeit und Fehler überprüfen. Die Aufgabe zur *Update-Prüfung* wird automatisch im Rahmen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausgeführt. Der Administrationsserver lädt Updates aus der Quelle herunter, speichert sie in einem temporären Verzeichnis und startet die Aufgabe zur *Update-Prüfung*. Wenn die Aufgabe erfolgreich ausgeführt wurde, werden die Updates von der temporären Datenverwaltung in den freigegebenen Ordner des Administrationsservers kopiert. Sie werden an alle Client-Geräte verteilt, für die der Administrationsserver als Update-Quellen dient.

Wenn in den Ergebnissen der Aufgabe zur *Update-Prüfung* die im temporären Verzeichnis liegenden Updates als fehlerhaft eingestuft werden oder wenn die Aufgabe zur *Update-Prüfung* mit einem Fehler beendet wird, werden die Updates nicht im freigegebenen Ordner gespeichert. Auf dem Administrationsserver verbleibt das vorherige Update. Dann werden auch die Aufgaben mit dem Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** nicht gestartet. Diese Vorgänge werden beim nächsten Ausführen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* gestartet, wenn die Prüfung der neuen Updates erfolgreich verläuft.

Das Update gilt als fehlerhaft, wenn mindestens ein Testgerät eine der folgenden Bedingungen erfüllt:

- Es ist ein Fehler in einer Update-Aufgabe aufgetreten.
- Nach Übernahme der Updates hat sich der Status des Echtzeitschutzes der Sicherheitsanwendung geändert.
- Während der Ausführung der Untersuchungsaufgabe auf Befehl wurde ein infiziertes Objekt gefunden.
- Es ist ein Funktionsfehler einer Kaspersky-Anwendung aufgetreten.

Wenn auf keinem Testgerät eine der genannten Bedingungen erfüllt wurde, wird das Set an Updates als ordnungsgemäß anerkannt und die Aufgabe zur *Update-Prüfung* gilt als erfolgreich abgeschlossen.

Bevor Sie mit der Erstellung der Aufgabe zur *Update-Prüfung* beginnen, führen Sie folgende Voraussetzungen aus:

1. Erstellen Sie eine Administrationsgruppe mit mehreren Testgeräten. Sie benötigen diese Gruppe, um die Updates zu prüfen.

   Es wird empfohlen Testgeräte zu verwenden, die gut geschützt sind und die eine Anwendungskonfiguration aufweisen, die im Unternehmensnetzwerk am weitesten verbreitet ist. Dieser Ansatz erhöht während der Untersuchung die Qualität und Wahrscheinlichkeit der Erkennung von Viren und minimiert das Risiko von Fehlalarmen. Wenn Viren auf Testgeräten gefunden werden, wird die Aufgabe zur *Update-Prüfung* als nicht erfolgreich betrachtet.

2. Erstellen Sie die Update-Aufgabe und die Aufgabe zur Schadsoftware-Untersuchung für eine von Kaspersky Security Center unterstützte Anwendung, z. B. Kaspersky Endpoint Security für Windows oder Kaspersky Security für Windows Server. Geben Sie beim Erstellen der Update-Aufgabe und der Aufgabe zur Schadsoftware-Untersuchung die Administrationsgruppe mit den Testgeräten an.

   Die Aufgabe zur *Update-Prüfung* führt die Update-Aufgabe und die Aufgabe zur Schadsoftware-Untersuchung auf den Testgeräten nacheinander aus, um zu überprüfen, ob alle Updates zulässig sind. Beim Erstellen der Aufgabe zur *Update-Prüfung*, müssen Sie zusätzlich die Update-Aufgabe und die Aufgabe zur Schadsoftware-Untersuchung angeben.

3. Erstellen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

Damit Kaspersky Security Center die empfangenen Updates überprüft, bevor sie auf die Client-Geräte verteilt werden, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers**.

3. Wechseln Sie im folgenden Fenster mit den Aufgabeneigenschaften zur Registerkarte **Programmeinstellungen** und aktivieren Sie anschließend die Option **Update-Prüfung ausführen**.

4. Wenn die Aufgabe zur *Update-Prüfung* existiert, klicken Sie auf die Schaltfläche **Aufgabe auswählen**. Wählen Sie im folgenden Fenster die Aufgabe zur *Update-Prüfung* in der Administrationsgruppe mit den Testgeräten aus.

5. Wenn Sie die Aufgabe zur *Update-Prüfung* noch nicht erstellt haben, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

   b. Geben Sie im folgenden Assistenten für das Erstellen einer Aufgabe einen Aufgabennamen an, wenn Sie den voreingestellten Namen ändern möchten.

   c. Wählen Sie die zuvor erstellte Administrationsgruppe mit den Testgeräten aus.

   d. Wählen Sie für ein erforderliches Programms, das von Kaspersky Security Center unterstützt wird, zunächst die Update-Aufgabe und anschließend die Aufgabe zur Schadsoftware-Untersuchung aus.

   Danach werden die folgenden Optionen angezeigt. Es wird empfohlen, diese aktiviert zu lassen:

   - **Gerät nach Datenbanken-Update neu starten**

     Nachdem die Antiviren-Datenbanken eines Gerät aktualisiert wurden, wird es empfohlen, das Gerät neu zu starten.

     Die Option ist standardmäßig aktiviert.

   - **Status des Echtzeitschutzes nach Datenbanken-Update und Geräteneustart überprüfen**

     Wenn diese Option aktiviert ist prüft die Aufgabe zur *Update-Prüfung*, ob die in die Datenverwaltung des Administrationsservers heruntergeladenen Updates zulässig sind und ob die Schutzstufe nach dem Update der Antiviren-Datenbanken und dem Neustart des Geräts gesunken ist.

     Diese Option ist standardmäßig aktiviert.

   e. Geben Sie ein Konto an, unter welchem die Aufgabe zur *Update-Prüfung* ausgeführt wird. Sie können Ihr Konto verwenden und die Option **Standardbenutzerkonto** aktiviert lassen. Alternativ können Sie angeben, dass die Aufgabe unter einem anderen Konto ausgeführt werden soll, welches über die erforderlichen Zugriffsrechte verfügt. Wählen Sie dazu die Option **Benutzerkonto festlegen** aus und geben Sie anschließend die Anmeldeinformationen für dieses Konto ein.

6. Klicken Sie auf **Speichern**, um das Eigenschaftenfenster der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zu schließen.

Die automatische Update-Prüfung ist aktiviert. Wenn Sie jetzt die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen, beginnt diese mit der Update-Prüfung.

Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

Die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* funktioniert nur auf Windows-Geräten als Verteilungspunkte. Geräte mit Verteilungspunkten unter Linux oder macOS können keine Updates von Kaspersky Update-Servern herunterladen. Wenn sich mindestens ein Linux- oder macOS-Gerät im Aufgabenbereich befindet, bekommt die Aufgabe den Status *Fehlgeschlagen*. Selbst wenn die Aufgabe auf allen Windows-Geräten erfolgreich abgeschlossen wurde, gibt sie auf den übrigen Geräten einen Fehler zurück.

Sie können die Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* für eine Administrationsgruppe erstellen. Diese Aufgabe wird für die Verteilungspunkte ausgeführt, die zur angegebenen Administrationsgruppe gehören.

Sie können diese Aufgabe zum Beispiel dann nutzen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.

Diese Aufgabe ist erforderlich, um Updates von Kaspersky-Update-Servern in die Datenverwaltung der Verteilungspunkte herunterzuladen. Die Liste der Updates enthält:

- Updates von Datenbanken und Softwaremodulen für Kaspersky-Sicherheitsanwendungen
- Updates der Kaspersky Security Centers-Komponenten
- Updates von Kaspersky-Sicherheitsanwendungen

Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

Wenn Verteilungspunkte über einen Proxyserver mit dem Internet verbunden sind, müssen Sie die entsprechenden Einstellungen in der Richtlinie des Administrationsagenten angeben.

*So erstellen Sie die Aufgabe **Updates in die Datenverwaltung der Verteilungspunkte herunterladen** für eine ausgewählte Administrationsgruppe:*

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center im Feld **Aufgabentyp** die Option **Updates in die Datenverwaltung der Verteilungspunkte herunterladen**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie eine Optionsschaltfläche, um die Administrationsgruppe, die Geräteauswahl oder die Geräte, für die Aufgabe gilt, festzulegen.
6. Wenn Sie im Schritt **Erstellung der Aufgabe abschließen** die Standardeinstellungen der Aufgabe ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.
7. Klicken Sie auf **Erstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste angezeigt.
8. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
9. Geben Sie auf der Registerkarte **Programmeinstellungen** im Fenster der Aufgabeneigenschaften die folgenden Einstellungen an:

   - **Update-Quellen**

     Als Update-Quelle für den Verteilungspunkt können die folgenden Ressourcen verwendet werden:

     - Kaspersky-Update-Server

       HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen.

Diese Variante ist standardmäßig festgelegt.

- Lokaler Ordner oder Netzwerkordner

  Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Ein Netzwerkordner kann ein FTP- oder HTTP-Server oder eine SMB-Freigabe sein. Für Netzwerkordner, die eine Authentifizierung erfordern, wird nur das SMB-Protokoll unterstützt. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

  Ein FTP- oder HTTP-Server oder ein Netzwerkordner, der von einer Update-Quelle verwendet wird, muss eine Ordnerstruktur (mit Updates) enthalten, die der Struktur entspricht, die bei Verwendung der Kaspersky-Update-Server erstellt wurde.

- **Ordner zum Speichern von Updates**

  Der Pfad zum angegebenen Ordner, in dem die bezogenen Updates gespeichert werden. Sie können den Pfad des angegebenen Ordners in die Zwischenablage kopieren. Für eine Gruppenaufgabe können Sie den Pfad eines angegebenen Ordners nicht ändern.

- **Diff-Dateien herunterladen**

  Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

  Diese Option ist standardmäßig deaktiviert.

- **Updates nach altem Schema herunterladen**

  Ab Version 14 lädt Kaspersky Security Center die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit die Anwendung die Updates mithilfe des neuen Schemas herunterladen kann, muss die Update-Quelle die Update-Dateien mit den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Update-Quelle die Update-Dateien mit Metadaten enthält, die nur mit dem alten Schema kompatibel sind, aktivieren Sie die Option **Updates nach altem Schema herunterladen**. Andernfalls schlägt die Aufgabe zum Update-Download fehl.

  Sie müssen diese Option beispielsweise aktivieren, wenn als Update-Quelle ein lokaler Ordner oder ein Netzwerkordner angegeben sind, und wenn die Updatedateien in diesem Ordner von einer der folgenden Anwendungen heruntergeladen wurden:

  - Kaspersky Update Utility

    Dieses Tool lädt Updates unter Verwendung des alten Schemas herunter.

  - Kaspersky Security Center 13.2 oder frühere Version

    Ein Verteilungspunkt kann beispielsweise so konfiguriert sein, dass er die Updates aus einem lokalen oder aus einem Netzwerkordner übernimmt. In diesem Fall können Sie Updates über einen Administrationsserver mit Internetverbindung herunterladen und die Updates anschließend im lokalen Ordner des Verteilungspunkts ablegen. Wenn der Administrationsserver in Version 13.2 oder früher ausgeführt wird, aktivieren Sie in der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* die Option **Updates nach altem Schema herunterladen**.

  Diese Option ist standardmäßig deaktiviert.

10. Erstellen Sie einen Zeitplan für den Aufgabenstart. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

- **Aufgabe starten**

  Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

  - **Manuell**

    Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

    Diese Variante ist standardmäßig ausgewählt.

  - **Alle n Minuten**

    Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

    Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

  - **Alle n Stunden**

    Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

    Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

  - **Alle n Tage**

    Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

    Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

  - **Nach Wochentagen**

    Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

    Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

  - **Monatlich**

    Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

    In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

    Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

  - **Monatlich, an angegebenen Tagen der gewählten Wochen**

    Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

    Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

    > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Abschluss einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

11. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.

Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Bei der Ausführung der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* werden die Datenbanken-Updates und Updates der Programm-Module aus der Update-Quelle heruntergeladen und im freigegebenen Ordner gespeichert. Die heruntergeladenen Updates werden nur von jenen Verteilungspunkten verwendet, die zur angegebenen Administrationsgruppe gehören und für die keine separate Aufgabe zum Update-Download festgelegt wurde.

Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center aktivieren und deaktivieren

Updates und Patches für den Administrationsserver können nur manuell installiert werden, nachdem durch den Administrator eine ausdrückliche Genehmigung erteilt wurde.

Die automatische Installation der Updates für Komponenten von Kaspersky Security Center wird standardmäßig bei der Installation des Administrationsagenten auf dem Gerät aktiviert. Sie können diese bei der Installation des Administrationsagenten oder später mithilfe einer Richtlinie deaktivieren.

Um die automatische Installation der Updates für Komponenten von Kaspersky Security Center bei der lokalen Installation des Administrationsagenten auf dem Gerät zu deaktivieren, gehen Sie wie folgt vor:

1. Starten Sie die lokale Installation des Administrationsagenten auf dem Gerät.
2. Deaktivieren Sie im Schritt **Erweiterte Einstellungen** das Kontrollkästchen **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**.
3. Folgen Sie den Anweisungen des Assistenten.

   Auf dem Gerät wird der Administrationsagent mit der deaktivierten automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center installiert. Sie können die automatische Installation später mithilfe einer der Richtlinie aktivieren.

Um die automatische Installation der Updates für Komponenten von Kaspersky Security Center bei der Installation des Administrationsagenten auf dem Gerät mittels Installationspaket zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Installationspakete**.
2. Klicken Sie auf das Paket **Kaspersky Security Center Administrationsagent <Versionsnummer>**.
3. Wechseln Sie im Eigenschaftenfenster zur Registerkarte **Einstellungen**.
4. Klicken Sie auf **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**, um die Funktion zu deaktivieren.

   Der Administrationsagent wird aus diesem Paket mit der deaktivierten automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center installiert. Sie können die automatische Installation später mithilfe einer der Richtlinie aktivieren.

Wenn bei der Installation des Administrationsagenten auf dem Gerät das Kontrollkästchen aktiviert (deaktiviert) war, können Sie die automatische Installation später mithilfe einer Richtlinie des Administrationsagenten deaktivieren (aktivieren).

Um die automatische Installation der Updates für Komponenten von Kaspersky Security Center mithilfe einer Richtlinie des Administrationsagenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie für Administrationsagenten.
3. Wechseln Sie im Eigenschaftenfenster der Richtlinie zur Registerkarte **Programmeinstellungen**.
4. Aktivieren oder deaktivieren Sie im Abschnitt **Verwaltung von Patches und Updates** das Kontrollkästchen **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**, um die automatische Installation zu aktivieren oder zu deaktivieren.
5. Aktivieren Sie das Schloss-Symbol (🔒) für diese Umschalttaste.

   Die Richtlinie wird auf die ausgewählten Geräte angewendet und die automatische Installation von Updates und Patches für die Komponenten von Kaspersky Security Center wird auf diesen Geräten aktiviert (deaktiviert).

Automatische Installation von Updates für Kaspersky Endpoint Security für Windows

Sie können das automatische Update für die Datenbanken und Programm-Module von Kaspersky Endpoint Security für Windows auf Client-Geräten konfigurieren.

So konfigurieren Sie den Download und die automatische Installation von Updates für Kaspersky Endpoint Security für Windows auf Geräten:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Endpoint Security für Windows die Variante **Update** als Untertyp der Aufgabe aus.
4. Geben Sie den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf höchstens 100 Zeichen lang sein und darf keine Sonderzeichen ("*<>?\:|) enthalten.
5. Wählen Sie den Aufgabenbereich aus.
6. Geben Sie die Administrationsgruppe, die Geräteauswahl oder die Geräte an, für welche die Aufgabe gilt.
7. Wenn Sie beim Schritt **Erstellung der Aufgabe abschließen** die Standardeinstellungen der Aufgabe ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.
8. Klicken Sie auf **Erstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste angezeigt.
9. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
10. Legen Sie auf der Registerkarte **Programmeinstellungen** im Fenster mit den Aufgabeneigenschaften die Einstellungen der Update-Aufgabe für den lokalen oder mobilen Modus fest:

    - **Lokaler Modus**: zwischen dem Gerät und Administrationsserver ist eine Verbindung hergestellt.
    - **Mobiler Modus**: zwischen Kaspersky Security Center und dem Gerät besteht keine Verbindung (wenn beispielsweise das Gerät nicht mit dem Internet verbunden ist).
11. Aktivieren Sie die Update-Quellen, die Sie verwenden möchten, um Datenbanken und Programm-Module für Kaspersky Endpoint Security für Windows zu aktualisieren. Bei Bedarf können Sie die Position der Quellen in der Liste ändern. Dafür gibt es die Schaltflächen **Nach oben** und **Nach unten**. Wenn mehrere Update-Quellen aktiviert sind, versucht Kaspersky Endpoint Security für Windows, sich anhand der Liste mit einer Quelle zu verbinden. Die Update-Aufgabe wird ausgeführt, indem das Update-Paket von der ersten verfügbaren Quelle abgerufen wird.
12. Aktivieren Sie die Option **Genehmigte Updates für Anwendungsmodule installieren**, um die Updates für Programm-Module zusammen mit den Programm-Datenbanken herunterzuladen und zu installieren.

Wenn diese Option aktiviert ist, benachrichtigt Kaspersky Endpoint Security für Windows den Benutzer über verfügbare Updates für Programm-Module und aktiviert während der Ausführung der Update-Aufgabe das Update der Programm-Module im Update-Paket. Kaspersky Endpoint Security für Windows installiert nur die Updates, für die Sie den Status *Genehmigt* festgelegt haben. Sie werden lokal über die Programmoberfläche oder über Kaspersky Security Center installiert.

Sie können auch die Option **Kritische Updates für Programm-Module automatisch installieren** aktivieren. Wenn Updates für Programm-Module verfügbar sind, installiert Kaspersky Endpoint Security für Windows automatisch alle Updates mit dem Status *Kritisch*. Die restlichen Updates werden installiert, nachdem Sie diese genehmigt haben.

Wenn es für ein Update der Programm-Module erforderlich ist, dass der Benutzer die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie liest und akzeptiert, werden die Updates erst installiert, nachdem der Benutzer die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie akzeptiert hat.

13. Aktivieren Sie das Kontrollkästchen **Updates in Ordner kopieren**, damit die Anwendung die heruntergeladenen Updates in einen Ordner kopiert, und geben Sie dann den Pfad an.

14. Planen Sie die Aufgabe. Um zeitnahe Updates sicherzustellen, wird empfohlen, die Option **Nach dem Download von Updates in die Datenverwaltung** zu aktivieren.

15. Klicken Sie auf **Speichern**.

Beim Ausführen der Aufgabe **Update** sendet die Anwendung Anfragen an die Kaspersky-Update-Server.

Einige Updates erfordern die Installation der neuesten Versionen von Verwaltungs-Plug-ins.

Genehmigen und Ablehnen von Software-Updates

Die Einstellungen einer Aufgabe zur Update-Installation erfordern eventuell die Genehmigung der zu installierenden Updates. Sie können Updates, die installiert werden müssen, genehmigen und Updates, die nicht installiert werden dürfen, ablehnen.

Beispielsweise können Sie die Update-Installation zuerst in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb der Geräte nicht stören, und erst anschließend die Installation dieser Updates auf Client-Geräten zulassen.

Das Genehmigen und Ablehnen von Updates ist nur für Administrationsagenten und verwaltete Anwendungen verfügbar, die auf Windows-basierten Client-Geräten installiert sind. Ein nahtloses Update der folgenden Komponenten wird nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung. Um diese Komponenten zu aktualisieren, müssen Sie die jeweils aktuellste Version von der Kaspersky-Website herunterladen und anschließend manuell installieren.

So genehmigen Sie ein oder mehrere Updates oder lehnen die Updates ab:

1. Gehen Sie im Hauptmenü zu **Vorgänge → Programme von Kaspersky → Nahtlose Updates**.

   Eine Liste der verfügbaren Updates wird geöffnet.

Für Updates von verwalteten Anwendungen muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center installiert sein. Wenn diese Version höher ist als Ihre aktuelle Version, werden diese Updates zwar angezeigt, können jedoch nicht genehmigt werden. Außerdem können aus solchen Updates keine Installationspakete erstellt werden, bevor Kaspersky Security Center nicht aktualisiert wurde. Sie werden aufgefordert, Ihre Kaspersky Security Center-Instanz auf die erforderliche Mindestversion zu aktualisieren.

2. Wählen Sie die Updates aus, die Sie genehmigen oder ablehnen möchten.

3. Klicken Sie auf **Genehmigen**, um die ausgewählten Updates zu genehmigen, oder auf **Ablehnen**, um die ausgewählten Updates abzulehnen.

   Der Standardwert ist *Nicht festgestellt*.

Die Updates, für die Sie den Status *Genehmigt* auswählen, werden in eine Warteschlange für die Installation verschoben.

Die Updates, für die Sie den Status *Abgelehnt* auswählen, werden von allen Geräten, auf denen sie bisher installiert waren, deinstalliert (falls möglich). Ferner werden sie in Zukunft nicht auf anderen Geräten installiert.

Einige Updates für die Kaspersky-Anwendungen können nicht deinstalliert werden. Wenn Sie den Status *Abgelehnt* für sie festlegen, wird Kaspersky Security Center diese Updates nicht von den Geräten deinstallieren, auf denen sie zuvor installiert waren. Diese Updates werden jedoch in Zukunft niemals auf anderen Geräten installiert.

Wenn Sie an Updates für Drittanbieter-Programme den Status *Abgelehnt* vergeben, werden diese Updates nicht auf jenen Geräten installiert, auf denen eine Installation vorgesehen war, aber noch nicht durchgeführt wurde. Auf den Geräten, auf denen die Updates bereits installiert sind, werden diese beibehalten. Wenn Sie solche Updates löschen müssen, können Sie dies lokal und manuell tun.

Aktualisieren des Administrationsservers

Zum Installieren von Administrationsserver-Updates dient der Assistent für das Update des Administrationsservers.

Um ein Administrationsserver-Update zu installieren:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Programme von Kaspersky → Nahtlose Updates**.

2. Der Assistent für das Update des Administrationsservers kann auf eine der folgenden Arten ausgeführt werden:

   - Klicken Sie in der Update-Liste auf den Namen eines Administrationsserver-Updates und klicken Sie im folgenden Fenster auf den Link **Assistent für das Update des Administrationsservers ausführen**.

   - Klicken Sie im Benachrichtigungsfeld im oberen Fensterbereich auf den Link **Assistent für das Update des Administrationsservers ausführen**.

3. Wählen Sie im Fenster Assistent für das Update des Administrationsservers eine der folgenden Optionen, um anzugeben, wann ein Update installiert werden soll:

   - **Jetzt installieren**. Wählen Sie diese Variante, wenn Sie das Update jetzt installieren möchten.
   - **Installation aufschieben**. Wählen Sie diese Variante, wenn Sie dieses Update später installieren möchten. In diesem Fall wird eine Benachrichtigung über dieses Update angezeigt.
   - **Dieses Update ignorieren**. Wählen Sie diese Option, wenn Sie ein Update nicht installieren und keine Benachrichtigungen über dieses Update erhalten möchten.

4. Aktivieren Sie die Option **Backup-Kopie des Administrationsservers vor der Installation des Updates anlegen**, wenn Sie vor der Update-Installation eine Sicherungskopie des Administrationsservers erstellen möchten.

5. Klicken Sie auf die Schaltfläche **OK**, um den Assistenten zu beenden.

Wenn der Sicherungsvorgang unterbrochen wird, wird auch der Update-Installationsvorgang unterbrochen.

Autonomes Modell für den Download von Updates aktivieren und deaktivieren

Es wird empfohlen, das autonome Modell für den Download von Updates nicht zu deaktivieren. Die Deaktivierung kann zu Störungen bei der Zustellung von Updates an die Geräte führen. In manchen Fällen wird der Experte des Technischen Supports von Kaspersky Ihnen eventuell empfehlen, die Option **Updates und Antiviren-Datenbanken vom Administrationsserver vorab herunterladen** zu deaktivieren. In einem solchen Fall müssen Sie sicherstellen, dass die Aufgabe zum Update-Download für Kaspersky-Anwendungen eingerichtet ist.

Um das autonome Modell zum Abrufen von Updates für die Administrationsgruppe zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

2. Klicken Sie auf die Schaltfläche **Gruppen**.

3. Wählen Sie in der Struktur die Administrationsgruppe, für die das autonome Modell zum Abrufen von Updates aktiviert werden soll.

4. Klicken Sie auf die Richtlinie für Administrationsagenten.

   Das Eigenschaftenfenster der Richtlinie des Administrationsagenten wird geöffnet.

   Standardmäßig werden die Einstellungen untergeordneter Richtlinien von übergeordneten Richtlinien geerbt und können nicht bearbeitet werden. Wenn die Richtlinie, die Sie bearbeiten möchten, geerbt ist, müssen Sie zunächst eine neue Richtlinie für den Administrationsagenten in der erforderlichen Administrationsgruppe erstellen. In der neu erstellten Richtlinie können Sie die Einstellungen bearbeiten, die in der übergeordneten Richtlinie nicht gesperrt sind.

5. Wählen Sie auf der Registerkarte **Programmeinstellungen** den Abschnitt **Verwaltung von Patches und Updates** aus.

6. Aktivieren oder deaktivieren Sie die Option **Updates und Antiviren-Datenbanken im Voraus vom Administrationsserver herunterladen (empfohlen)**, um das autonome Modell für den Download von Updates zu aktivieren oder zu deaktivieren.

   Das autonome Modell für den Download von Updates ist standardmäßig aktiviert.

Das autonome Modell für den Download von Updates wird daraufhin aktiviert oder deaktiviert.

Datenbanken und Software-Module von Kaspersky auf autonomen Geräten aktualisieren

Das Durchführen von Updates der Kaspersky-Datenbanken und Programm-Module auf verwalteten Geräten ist eine wichtige Aufgabe, um den Schutz gegen Viren und andere Bedrohungen aufrechtzuerhalten. In der Regel konfigurieren Administratoren regelmäßige Updates durch die Nutzung der Datenverwaltungen des Administrationsservers oder der Verteilungspunkte.

Wenn Sie Updates von Datenbanken und Programm-Modulen auf einem Gerät (oder auf einer Gruppe von Geräten) durchführen müssen, die nicht mit dem Administrationsserver (primär oder sekundär), einem Verteilungspunkt oder dem Internet verbunden sind, müssen Sie eine alternative Update-Quelle, wie einen FTP-Server oder einen lokalen Ordner, nutzen. In diesem Fall müssen Sie die für die Updates benötigten Dateien über ein Massenspeichergerät, wie beispielsweise ein USB-Stick oder eine externe Festplatte, bereitstellen.

Kopieren Sie die benötigten Updates vom:

- Administrationsserver.

  Um sicherzustellen, dass die Datenverwaltung des Administrationsservers über die, von der auf dem autonomen Gerät installierten Sicherheitsanwendung benötigten, Updates verfügt, muss auf mindestens einem der verwalteten Online-Geräte die gleiche Sicherheitsanwendung installiert sein. Diese Anwendung muss so angepasst sein, dass sie mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers die Updates aus der Datenverwaltung des Administrationsservers erhält.

- Jedes Gerät, dass die gleiche Sicherheitsanwendung installiert und so konfiguriert hat, dass sie Updates aus den Datenverwaltungen des Administrationsservers oder der Verteilungspunkte, oder direkt von den Kaspersky-Servern erhält.

Unten befindet sich ein Beispiel zur Update-Konfiguration von Datenbanken und Programm-Modulen, in welcher die Updates aus der Datenverwaltung des Administrationsservers kopiert werden.

So aktualisieren Sie Kaspersky-Datenbanken und Programm-Module auf autonomen Geräten:

1. Verbinden Sie einen Wechseldatenträger mit dem Gerät, auf dem der Administrationsserver installiert ist.

2. Kopieren Sie die Update-Dateien auf den Wechseldatenträger.

   Standardmäßig befinden sich die Updates unter: \\<Servername>\KLSHARE\Updates.

   Alternativ können Sie Kaspersky Security Center so konfigurieren, dass es die Updates regelmäßig in einen von Ihnen gewählten Ordner kopiert. Verwenden Sie dazu die Option **Heruntergeladene Updates in zusätzliche Ordner kopieren** in den Eigenschaften der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers. Wenn Sie einen Ordner auf einem USB-Stick oder einer externen Festplatte als Zielordner für diese Option angeben, wird dieses Massenspeichergerät stets über die aktuellsten Versionen der Updates verfügen.

3. Konfigurieren Sie auf autonomen Geräten die Sicherheitsanwendungen (zum Beispiel Kaspersky Endpoint Security für Windows) so, dass sie Updates aus einem lokalen Ordner oder von einer gemeinsam genutzten Ressource, wie ein FTP-Server oder einem gemeinsamer Ordner, erhalten.

4. Kopieren Sie die Update-Dateien von dem Wechseldatenträger in den lokalen Ordner oder auf die gemeinsam genutzte Ressource, die Sie als Update-Quelle nutzen wollen.

5. Starten Sie die Update-Aufgabe von Kaspersky Endpoint Security für Windows auf dem autonomen Gerät, das die Installation von Updates benötigt.

Nachdem die Update-Aufgabe abgeschlossen wurde, sind die Kaspersky-Datenbanken und Programm-Module auf diesem Gerät auf dem neuesten Stand.

Web-Plugins sichern und wiederherstellen

Mit Kaspersky Security Center Web Console können Sie den aktuellen Zustand eines Web-Plug-ins sichern, um den gespeicherten Zustand später wiederherstellen zu können. Beispielsweise können Sie ein Web-Plug-in sichern, bevor Sie es auf eine neuere Version aktualisieren. Wenn die neuere Version nach dem Update nicht Ihren Anforderungen oder Erwartungen entspricht, können Sie die vorherige Version des Web-Plug-ins aus dem Backup wiederherstellen.

So sichern Sie Web-Plug-Ins:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Web-Plug-ins**.

2. Wählen Sie im Abschnitt **Web-Plug-ins** die Web-Plug-ins aus, die Sie sichern möchten, und klicken Sie anschließend auf die Schaltfläche **Backup-Kopie erstellen**.

Die ausgewählten Web-Plug-ins werden gesichert. Sie können die erstellten Backups im Abschnitt **Backups** anzeigen.

So stellen Sie ein Web-Plug-in aus einem Backup wieder her:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Backups**.

2. Wählen Sie im Abschnitt **Backups** das Backup von dem Web-Plug-in aus, welches Sie wiederherstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Aus Backup wiederherstellen**.

Das Web-Plug-in wird aus dem ausgewählten Backup wiederhergestellt.

Verteilungspunkte und Verbindungs-Gateways anpassen

Die Struktur der Administrationsgruppen in Kaspersky Security Center erfüllt folgende Funktionen:

- Gültigkeitsbereich der Richtlinien festlegen

  Mithilfe von *Richtlinienprofilen* existiert eine alternative Möglichkeit, um die notwendigen Einstellungen auf den Geräten anzuwenden. In diesem Fall legen Sie den Gültigkeitsbereich der Richtlinien mithilfe von Tags, des Speicherorts der Geräte in den Active Directory-Verzeichnissen, oder der Zugehörigkeit zu den Active Directory-Sicherheitsgruppen fest.

- Gültigkeitsbereich der Gruppenaufgaben festlegen

  Es gibt eine Methode zur Festlegung des Gültigkeitsbereichs der Gruppenaufgaben, die nicht auf der Hierarchie der Administrationsgruppen basiert: die Nutzung von Aufgaben für die Geräteauswahlen und eine Reihe von Geräten.

- Festlegung der Zugriffsrechte auf die Geräte, sowie auf die virtuellen und sekundären Administrationsserver

- Weist Verteilungspunkte zu

Beim Aufbau der Struktur der Administrationsgruppen muss für eine optimale Bestimmung der Verteilungspunkte die Netzwerktopologie des Unternehmens berücksichtigt werden. Die optimale Zuordnung der Verteilungspunkte ermöglicht eine Verringerung des Netzwerkverkehrs innerhalb des Unternehmensnetzwerks.

Abhängig von der planmäßigen Struktur des Unternehmens und der Topologie der Netzwerke können die folgenden typischen Konfigurationen für die Struktur der Administrationsgruppen unterschieden werden:

- Einzelbüro

- Mehrere kleine, eigenständige Büros

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Typische Konfiguration von Verteilungspunkten: Einzelbüro

In einer typischen Einzelbüro-Konfiguration befinden sich alle Geräte im Netzwerk des Unternehmens und können einander "sehen". Das Netzwerk des Unternehmens kann aus mehreren ausgewählten Teilen (der Netzwerke oder der Netzwerksegmente) bestehen, die über enge Kanäle verbunden sind.

Es sind die folgenden Methoden für den Aufbau der Struktur der Administrationsgruppen möglich:

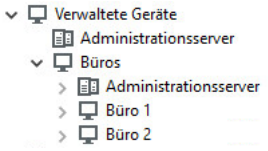
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen. Die Verteilungspunkte können automatisch bestimmt oder manuell zugewiesen werden.

- Aufbau der Struktur der Administrationsgruppen, in der die Netztopologie nicht widergespiegelt wird. In diesem Fall müssen Sie die automatische Bestimmung der Verteilungspunkte deaktivieren und dann für die Stammadministrationsgruppe in jedem ausgewählten Teil des Netzwerkes ein oder mehrere Geräte als Verteilungspunkte bestimmen, beispielsweise für die Gruppe **Verwaltete Geräte**. Alle Verteilungspunkte befinden sich dann auf einer Ebene und haben den identischen Gültigkeitsbereich, der alle Geräte im Netzwerk des Unternehmens umfasst. Jeder Administrationsagent wird in diesem Fall mit dem Verteilungspunkt verbunden, zu dem die Route am kürzesten ist. Die Route zum Verteilungspunkt kann mithilfe des Tools "tracert" bestimmt werden.

Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros

Diese typische Konfiguration entspricht einer Menge kleiner Remote-Büros, die eventuell durch das Internet mit dem Hauptbüro verbunden sind. Jedes der Remote-Büros befindet sich hinter einer NAT. Das bedeutet, dass ein Remote-Büro nicht mit einem anderen verbunden werden kann und die Büros voneinander isoliert sind.

Diese Konfiguration muss in der Struktur der Administrationsgruppen widergespiegelt werden: für jedes Remote-Büro muss eine separate Administrationsgruppe erstellt werden (entspr. Gruppen **Büro 1**, **Büro 2** auf der nachfolgenden Abbildung).



Die Remote-Büros werden in der Struktur der Administrationsgruppen abgebildet.

Für jede Administrationsgruppe, die einem Büro entspricht, müssen ein oder mehrere Verteilungspunkte festgelegt werden. Als Verteilungspunkte müssen Geräte des Remote-Büros bestimmt werden, die genug freien Platz auf dem Datenträger haben. Die Geräte, die sich beispielsweise in der Gruppe **Büro 1** befinden, wenden sich an die Verteilungspunkte, die für die Administrationsgruppe **Büro 1** bestimmt wurden.

Wenn einige Benutzer samt ihren Laptops physisch zwischen Büros wechseln, müssen in jedem Remote-Büro zusätzlich zu den oben erwähnten Verteilungspunkten zwei oder mehrere Geräte ausgewählt und als Verteilungspunkte für die Administrationsgruppe der obersten Ebene bestimmt werden (Gruppe **Stammgruppe für die Büros** in der obigen Abbildung).

Beispiel: Es gibt einen Laptop, der sich in der Administrationsgruppe **Büro 1** befindet, aber physisch in ein Büro gebracht wird, das der Gruppe **Büro 2** entspricht. Nach dem Ortswechsel versucht der Administrationsagent auf dem Laptop, sich an die Verteilungspunkte zu wenden, die zur Gruppe **Büro 1** gehören. Diese Verteilungspunkte erweisen sich allerdings als nicht verfügbar. Dann beginnt der Administrationsagent, sich an die Verteilungspunkte zu wenden, die für die Gruppe **Stammgruppe für die Büros** bestimmt wurden. Da die Remote-Büros voneinander isoliert sind, werden von allen Verteilungspunkten, die für die Administrationsgruppe **Stammgruppe für die Büros** bestimmt wurden, nur die Zugriffe des Administrationsagenten auf die Verteilungspunkte erfolgreich sein, die für die Gruppe **Büro 2** bestimmt wurden. Das bedeutet, dass der Laptop zwar in der Administrationsgruppe bleibt, die dem ursprünglichen Büro entspricht, aber die Verteilungspunkte jenes Büros verwendet, in dem er sich in diesen Moment physisch befindet.

Über das Zuweisen von Verteilungspunkten

Sie können einem verwalteten Gerät entweder manuell oder automatisch die Funktion des Verteilungspunkts zuweisen.

Wenn Sie einem verwalteten Gerät die Funktion des Verteilungspunkts manuell zuweisen, können Sie ein beliebiges Gerät in Ihrem Netzwerk auswählen.

Wenn Sie die Funktion des Verteilungspunkts automatisch zuweisen, kann Kaspersky Security Center nur ein verwaltetes Gerätes auswählen, das die folgenden Bedingungen erfüllt:

- Es sind mindestens 50 GB freier Speicherplatz auf dem Datenträger vorhanden.
- Das verwaltete Gerät ist direkt mit Kaspersky Security Center verbunden (nicht über das Gateway).
- Das verwaltete Gerät ist kein Laptop.

> Wenn Ihr Netzwerk kein Gerät enthält, das die angegebenen Bedingungen erfüllt, weist Kaspersky Security Center keinem Gerät die Funktion des Verteilungspunkts automatisch zu.

Verteilungspunkte automatisch zuweisen

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. In diesem Fall wählt Kaspersky Security Center die Geräte, die zu Verteilungspunkten bestimmt werden, selbständig aus.

Um Verteilungspunkte automatisch zuzuweisen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Wählen Sie die Option **Verteilungspunkte automatisch zuweisen** aus.

   Wenn die automatische Gerätezuweisung für Verteilungspunkte aktiviert ist, können die Einstellungen der Verteilungspunkte nicht manuell angepasst werden und die Liste der Verteilungspunkte kann nicht verändert werden.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Daraufhin beginnt der Administrationsserver damit, Verteilungspunkte automatisch zu bestimmen und ihre Einstellungen zu konfigurieren.

Verteilungspunkte manuell zuweisen

In Kaspersky Security Center haben Sie die Möglichkeit, Geräte manuell zu Verteilungspunkten zu bestimmen.

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. In diesem Fall wählt Kaspersky Security Center die Geräte, die zu Verteilungspunkten bestimmt werden, selbständig aus. Wenn Sie jedoch aus bestimmten Gründen auf die automatische Bestimmung der Verteilungspunkte verzichten möchten (beispielsweise wenn Sie speziell ausgewählte Server verwenden wollen), können Sie die Verteilungspunkte manuell bestimmen, nachdem Sie deren Anzahl und Konfiguration berechnet haben.

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Um ein Gerät manuell zum Verteilungspunkt zu bestimmen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Wählen Sie die Option **Verteilungspunkte manuell zuweisen** aus.

4. Klicken Sie auf die Schaltfläche **Zuweisen**.

5. Wählen Sie das Gerät aus, das Sie zu einem Verteilungspunkt machen möchten.

   Berücksichtigen Sie bei der Auswahl des Geräts die Besonderheiten des Verteilungspunkts und die Anforderungen an das Gerät, das die Rolle des Verteilungspunkts übernehmen soll.

6. Wählen Sie die Administrationsgruppe aus, die zum Gültigkeitsbereich des ausgewählten Verteilungspunkts gehören soll.

7. Klicken Sie auf die Schaltfläche **OK**.

   Der hinzugefügte Verteilungspunkt wird in der Liste der Verteilungspunkte im Abschnitt **Verteilungspunkte** angezeigt.

8. Klicken Sie den hinzugefügten Verteilungspunkt in der Liste an, um sein Eigenschaftenfenster zu öffnen.

9. Passen Sie im Eigenschaftenfenster die Einstellungen des Verteilungspunkts an:

   - Der Abschnitt **Allgemein** enthält die Einstellung für die Interaktion des Verteilungspunkts mit den Client-Geräten:

     - **SSL-Port**

       Nummer des SSL-Ports, über den die geschützte Verbindung des Client-Geräts mit dem Verteilungspunkt über das SSL-Protokoll erfolgt.

       Standardmäßig ist die Portnummer 13000 festgelegt.

     - **Multicast verwenden**

       Wenn diese Option aktiviert ist, werden die Installationspakete automatisch mithilfe von IP-Multicasting an die Client-Geräte innerhalb einer Gruppe verteilt.

       IP-Multicasting erhöht die Dauer für die Installation einer Anwendung aus einem Installationspaket in eine Gruppe von Client-Geräten. Dagegen reduziert es die Installationsdauer, wenn Sie eine Anwendung auf einem einzelnen Client-Gerät installieren.

     - **Adresse für IP-Multicast**

       IP-Adresse, die für das Multicasting verwendet wird. Die IP-Adresse kann man im Bereich 224.0.0.0 – 239.255.255.255 festgelegt werden.

       Standardmäßig weist Kaspersky Security Center automatisch eine eindeutige IP-Multicast-Adresse im angegeben Bereich zu.

     - **Portnummer für IP-Multicast**

       Portnummer für das IP-Multicasting.

       Standardmäßig wird Port 15001 verwendet. Wenn als Verteilungspunkt ein Gerät angegeben wurde, auf dem der Administrationsserver installiert ist, wird für die Verbindung mit dem SSL-Protokoll standardmäßig Port 13001 verwendet.

     - **Adresse des Verteilungspunkts für Remote-Geräte**

       Die Netzwerkadresse, über die Remote-Geräte eine Verbindung zum Verteilungspunkt herstellen.

- **Updates verteilen**

  Aus den folgenden Quellen werden Updates an verwaltete Geräte verteilt:

  - Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
  - Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

  Wenn Sie zur Bereitstellung von Updates Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

  Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Update-Downloads und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

- **Installationspakete verteilen**

  Aus den folgenden Quellen werden Installationspakete an verwaltete Geräte verteilt:

  - Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
  - Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

  Wenn Sie zur Bereitstellung von Installationspaketen Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

  Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Downloads von Installationspaketen und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

- **Push-Server ausführen**

  In Kaspersky Security Center kann ein Verteilungspunkt als Push-Server für Geräte fungieren, die über das mobile Protokoll oder über den Administrationsagenten verwaltet werden. Ein Push-Server muss beispielsweise aktiviert sein, wenn Sie die erzwungene Synchronisierung von KasperskyOS-Geräten mit dem Administrationsserver verwenden möchten. Ein Push-Server besitzt denselben Umfang verwalteter Geräte wie der Verteilungspunkt, auf dem der Push-Server aktiviert ist. Wenn Sie mehrere Verteilungspunkte derselben Administrationsgruppe zugewiesen haben, können Sie den Push-Server auf jedem der Verteilungspunkte aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

- **Port des Push-Servers**

  Die Portnummer des Push-Servers. Sie können die Nummer eines beliebigen unbelegten Ports angeben.

- Geben Sie im Abschnitt **Bereich** den Bereich an, auf den der Verteilungspunkt die Updates verteilen soll (Administrationsgruppen und/oder Netzwerkspeicherort).

  Nur Geräte unter der Verwaltung von Windows können ihren Netzwerkspeicherort ermitteln. Die Bestimmung des Netzwerkspeicherorts ist für Geräte unter der Verwaltung anderer Betriebssysteme nicht verfügbar.

- Wenn der Verteilungspunkt auf einem anderen Computer als dem Administrationsserver ausgeführt wird, können Sie im Abschnitt **Update-Quelle** eine Updatequelle für den Verteilungspunkt auswählen:

  - **Update-Quelle**

    Wählen Sie eine Update-Quelle für den Verteilungspunkt aus:

    - Damit der Verteilungspunkt die Updates vom Administrationsserver erhält, wählen Sie **Vom Administrationsserver beziehen**.

    - Damit Verteilungspunkte Updates anhand einer Aufgabe beziehen können, wählen Sie **Aufgaben zum Update-Download verwenden** aus und geben Sie anschließend eine Aufgabe vom Typ *Download von Updates in die Datenverwaltung der Verteilungspunkte* an:

      - Wenn eine solche Aufgabe bereits auf dem Gerät vorhanden ist, wählen Sie die Aufgabe in der Liste aus.

      - Wenn auf dem Gerät noch keine derartige Aufgabe vorhanden ist, klicken Sie auf den Link **Aufgabe erstellen**, um eine Aufgabe zu erstellen. Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

  - **Diff-Dateien herunterladen**

    Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

    Diese Option ist standardmäßig aktiviert.

- Wenn Ihre Verteilungspunkte für die Verbindung mit dem Internet einen Proxyserver verwenden, können Sie im Unterabschnitt **Einstellungen für die Internetverbindung** die folgenden Einstellungen festlegen:

  - **Proxyserver verwenden**

    Wenn Sie das Kontrollkästchen aktivieren, können Sie in den Eingabefeldern die Verbindungseinstellungen zum Proxyserver angeben.

    Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

  - **Proxyserver-Adresse**

    Proxyserver-Adresse.

  - **Portnummer**

    Nummer des Ports, über den die Verbindung erfolgt.

  - **Proxyserver für lokale Adressen umgehen**

    Wenn die Option aktiviert ist, wird bei der Verbindung mit den Geräten im lokalen Netzwerk kein Proxyserver verwendet.

    Diese Option ist standardmäßig deaktiviert.

  - **Authentifizierung am Proxyserver**

    Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

    Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Benutzername**

  Benutzerkonto, unter dessen Namen die Verbindung mit dem Proxy-Server hergestellt wird.

- **Kennwort**

  Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

- Im Abschnitt **KSN Proxy** können Sie die Anwendung anpassen, um den Verteilungspunkt zum Weiterleiten von KSN-Anfragen von den verwalteten Geräten zu verwenden:

  - **KSN Proxy auf dem Verteilungspunkt aktivieren**

    Der KSN-Proxy-Service wird auf dem Gerät ausgeführt, das als Verteilungspunkt verwendet wird. Verwenden Sie diese Funktion, um Datenverkehr im Netzwerk neu zu verteilen und zu optimieren.

    Der Verteilungspunkt sendet die KSN-Statistik, die in der Erklärung zu Kaspersky Security Network aufgeführt sind, an Kaspersky.

    Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn im Fenster mit den Eigenschaften des Administrationsservers die Optionen **Administrationsserver als Proxyserver verwenden** und **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** aktiviert sind.

    Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

  - **KSN-Anfragen an den Administrationsserver weiterleiten**

    Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an den Administrationsserver weiter.

    Diese Option ist standardmäßig aktiviert.

  - **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**

    Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an die KSN Cloud oder an KPSN weiter. KSN-Anfragen, die der Verteilungspunkt selbst generiert, werden ebenso direkt an KSN Cloud oder KPSN gesendet.

    Verteilungspunkte, auf denen der Administrationsagent bis einschließlich Version 11 installiert ist, können nicht direkt auf KPSN zugreifen. Um die Verteilungspunkte so anzupassen, dass KSN-Anfragen an KPSN gesendet werden, aktivieren Sie für jeden Verteilungspunkt die Option **KSN-Anfragen an den Administrationsserver weiterleiten**.

    Verteilungspunkte, auf denen der Administrationsagent ab Version 12 installiert ist, können direkt auf KPSN zugreifen.

  - **Proxyserver-Einstellungen beim Verbinden mit KPSN ignorieren**

    Aktivieren Sie diese Option, wenn Sie die Proxyserver-Einstellungen in den Eigenschaften des Verteilungspunkts oder in der Richtlinie des Administrationsagenten angepasst haben, aber Ihre Netzwerkarchitektur eine direkte Verwendung von KPSN erfordert. Andernfalls können Anfragen von den verwalteten Apps KPSN nicht erreichen.

    Diese Option ist verfügbar, wenn Sie die Option **Direkt über das Internet auf KSN Cloud/KPSN zugreifen** auswählen.

  - **Port**

    Die Nummer des TCP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Standardmäßig wird Portnummer 13111 verwendet.

- **UDP-Port verwenden**

  Wenn es erforderlich ist, dass sich die verwalteten Geräte über einen UDP-Port mit dem KSN-Proxyserver verbinden, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine UDP-Portnummer an. Diese Option ist standardmäßig aktiviert.

- **UDP-Port**

  Die Nummer des UDP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Der standardmäßige UDP-Port für die Verbindung zum KSN-Proxyserver ist 15111.

- Wenn der Verteilungspunkt auf einem anderen Computer als dem Administrationsserver ausgeführt wird, können Sie im Abschnitt **Verbindungs-Gateway** den Verteilungspunkt so konfigurieren, dass er als Gateway für die Verbindung zwischen den Instanzen der Administrationsagenten und dem Administrationsserver fungiert:

  - **Verbindungs-Gateway**

    Wenn aufgrund der Organisation Ihres Netzwerks keine direkte Verbindung zwischen dem Administrationsserver und den Administrationsagenten hergestellt werden kann, können Sie den Verteilungspunkt als Verbindungs-Gateway zwischen Administrationsserver und Administrationsagenten verwenden.

    Aktivieren Sie diese Option, wenn der Verteilungspunkt als Verbindungs-Gateway zwischen den Administrationsagenten und dem Administrationsserver fungieren soll. Diese Option ist standardmäßig deaktiviert.

  - **Verbindung zum Gateway ausgehend vom Administrationsserver herstellen (falls sich das Gateway in der DMZ befindet)**

    Wenn sich der Administrationsserver außerhalb der demilitarisierten Zone (DMZ) in einem lokalen Netzwerk befindet, können auf Remote-Geräten installierte Administrationsagenten keine Verbindung zum Administrationsserver herstellen. Sie können einen Verteilungspunkt als Verbindungs-Gateway mit Reverse Connectivity verwenden (der Administrationsserver stellt eine Verbindung zum Verteilungspunkt her).

    Aktivieren Sie diese Option, wenn Sie den Administrationsserver mit dem Verbindungs-Gateway in der DMZ verbinden müssen.

  - **Lokalen Port für Kaspersky Security Center Web Console öffnen**

    Aktivieren Sie diese Option, wenn Sie das Verbindungs-Gateway in der DMZ benötigen, um einen Port für die Web Console zu öffnen, der sich in der DMZ oder im Internet befindet. Geben Sie die Portnummer an, die für die Verbindung von der Web Console zum Verteilungspunkt verwendet wird. Standardmäßig wird Portnummer 13299 verwendet.

    Diese Option ist verfügbar, wenn Sie die Option **Verbindung zum Gateway ausgehend vom Administrationsserver herstellen (falls sich das Gateway in der DMZ befindet)** aktivieren.

  Wenn Sie mobile Geräte über den Verteilungspunkt, der als Verbindungs-Gateway fungiert, mit dem Administrationsserver verbinden, können Sie die folgenden Optionen aktivieren:

  - **Port für mobile Geräte öffnen (nur SSL-Authentifizierung des Administrationsservers)**

    Aktivieren Sie diese Option, wenn das Verbindungs-Gateway einen Port für mobile Geräte öffnen soll, und geben Sie die Portnummer an, die mobile Geräte für die Verbindung zum Verteilungspunkt verwenden. Standardmäßig wird Portnummer 13292 verwendet. Das mobile Gerät überprüft das Zertifikat des Administrationsservers. Beim Verbindungsaufbau wird nur der Administrationsserver authentifiziert.

- **Port für mobile Geräte öffnen (bidirektionale SSL-Authentifizierung)**

  Aktivieren Sie diese Option, wenn Sie ein Verbindungs-Gateway benötigen, um einen Port zu öffnen, der für die bidirektionale Authentifizierung des Administrationsservers und mobiler Geräte verwendet wird. Das mobile Gerät überprüft das Zertifikat des Administrationsservers und der Administrationsserver überprüft das Zertifikat des mobilen Geräts. Geben Sie die folgenden Parameter an:

  - Portnummer, die mobile Geräte für die Verbindung mit dem Verteilungspunkt verwenden. Standardmäßig wird Portnummer 13293 verwendet.

  - DNS-Domänennamen des Verbindungs-Gateways, die von mobilen Geräten verwendet werden. Trennen Sie Domänennamen durch Kommas. Die angegebenen Domänennamen werden in das Zertifikat des Verteilungspunkts aufgenommen. Wenn die von den mobilen Geräten verwendeten Domänennamen nicht mit dem allgemeinen Namen im Verteilungspunktzertifikat übereinstimmen, stellen die mobilen Geräte keine Verbindung zum Verteilungspunkt her.

    Standardmäßig entspricht der DNS-Domänenname dem FQDN-Namen des Verbindungsgateways.

  In beiden Fällen werden die Zertifikate nur während des Aufbaus der TLS-Sitzung auf dem Verteilungspunkt überprüft. Die Zertifikate werden nicht zur Prüfung durch den Administrationsserver weitergeleitet. Nachdem eine TLS-Sitzung mit dem mobilen Gerät hergestellt wurde, verwendet der Verteilungspunkt das Zertifikat des Administrationsservers, um einen Tunnel für die Synchronisierung zwischen dem mobilen Gerät und dem Administrationsserver herzustellen. Wenn Sie den Port für die bidirektionale SSL-Authentifizierung öffnen, kann das Zertifikat für mobile Geräte nur mithilfe eines Installationspakets verteilt werden.

- Passen Sie die Einstellungen für die Abfrage der Windows-Domänen, des Active Directory oder des IP-Bereichs für den Verteilungspunkt an:

  - **Windows-Domänen**

    Sie können für Windows-Domänen die Gerätesuche erlauben und den Zeitplan für die Abfrage festlegen.

  - **Domänencontroller**

    Sie können für Active Directory die Netzwerkabfrage erlauben und den Zeitplan für die Abfrage festlegen.

    Wenn Sie einen Windows-Verteilungspunkt verwenden, können Sie eine der folgenden Optionen auswählen:

    - **Aktuelle Domäne des Active Directory abfragen**.

    - **Domänengesamtstruktur des Active Directory abfragen**.

    - **Angegebene Domänen des Active Directory abfragen**. Wenn Sie diese Option auswählen, fügen Sie eine oder mehrere Active Directory-Domänen zur Liste hinzu.

    Wenn Sie einen Linux-Verteilungspunkt mit installiertem Administrationsagenten Version 15 verwenden, können Sie nur Active Directory-Domänen abfragen, für die Sie die Adresse und die Anmeldeinformationen des Benutzers angeben. Die Abfrage der aktuellen Active Directory-Domäne und der Active Directory-Domänen-Gesamtstruktur ist nicht verfügbar.

    Sie können für Domänencontroller die Gerätesuche aktivieren.

    Wenn Sie die Option **Abfrage des Domänencontrollers aktivieren** auswählen, können Sie Domänencontroller für die Abfrage auswählen und deren Abfragezeitplan festlegen.

    Wenn Sie einen Linux-Verteilungspunkt verwenden, klicken Sie im Abschnitt **Angegebene Domänen abfragen** auf **Hinzufügen** und geben Sie anschließend die Adresse und die Anmeldeinformationen des Domänencontrollers an.

Wenn Sie einen Windows-Verteilungspunkt verwenden, können Sie eine der folgenden Optionen auswählen:

- **Aktuelle Domäne abfragen**
- **Domänengesamtstruktur abfragen**
- **Angegebene Domänen abfragen**

- **IP-Bereiche**

  Sie können die Gerätesuche für IPv4-Bereiche und IPv6-Netzwerke aktivieren.

  Wenn Sie die Option **Abfrage des Bereichs zulassen** aktivieren, können Sie zu untersuchende Bereiche hinzufügen und den Zeitplan für sie festlegen. Sie können IP-Bereich zur Liste der untersuchten Bereiche hinzufügen.

  Wenn Sie die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** aktiviert haben, fragt der Verteilungspunkt das IPv6-Netzwerk automatisch unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. In diesem Fall werden angegebene IP-Bereiche ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt. Für Verteilungspunkte mit Linux ist die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** verfügbar. Um die Zeroconf IPv6-Abfrage verwenden zu können, müssen Sie das Tool "avahi-browser" auf dem Verteilungspunkt installieren.

- Geben Sie im Abschnitt **Erweitert** den Ordner an, den der Verteilungspunkt zum Speichern der zu verteilenden Daten verwenden soll:

  - **Standardordner verwenden**

    Bei Auswahl dieser Option wird zum Speichern der Ordner auf dem Verteilungspunkt verwendet, in dem der Administrationsagent installiert wurde.

  - **Benutzerdefinierten Ordner verwenden**

    Bei Auswahl dieser Option können Sie im unteren Feld den Pfad zum Ordner angeben. Dabei können Sie einen lokalen Ordner des Verteilungspunkts oder einen Ordner auf einem beliebigen, sich im Unternehmensnetzwerk befindlichen Remote-Gerät angeben.

    Das Benutzerkonto, unter dem der Administrationsagent auf dem Verteilungspunkt gestartet wird, muss über die Lese- und Schreibberechtigungen für den angegebenen Ordner verfügen.

10. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin übernehmen die ausgewählten Geräte die Rolle des Verteilungspunkts.

Liste mit Verteilungspunkten für eine Administrationsgruppe bearbeiten

Sie können eine Liste mit Verteilungspunkten anzeigen, die einer bestimmten Administrationsgruppe zugewiesen wurden, und Verteilungspunkte zu dieser Liste hinzufügen oder daraus löschen.

Um die Liste mit Verteilungspunkten, die einer Administrationsgruppe zugewiesen wurden, zu bearbeiten, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte auf den Pfad-Link.

3. Wählen Sie im geöffneten linken Bereich eine Administrationsgruppe aus, für welche Sie die zugewiesenen Verteilungspunkte ansehen möchten.

   Dadurch wird der Menüpunkt **Verteilungspunkte** aktiviert.

4. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verteilungspunkte**.

5. Um der Administrationsgruppe neue Verteilungspunkte hinzuzufügen, klicken Sie oberhalb der Liste der verwalteten Geräte auf die Schaltfläche **Zuweisen** und wählen Sie im angezeigten Fenster die Geräte aus.

6. Um die zugewiesenen Verteilungspunkte zu entfernen, wählen Sie Geräte aus der Liste aus und klicken Sie auf die Schaltfläche **Zuweisen aufheben**.

Je nach Ihren Änderungen werden neue Verteilungspunkte zur Liste hinzugefügt oder bestehende Verteilungspunkte daraus entfernt.

Erzwungene Synchronisierung

Obwohl Kaspersky Security Center Status, Einstellungen, Aufgaben und Richtlinien für verwaltete Geräte automatisch synchronisiert werden, möchten Sie vielleicht in einigen Fällen die Synchronisierung für ein bestimmtes Gerät erzwingen. Sie können die erzwungene Synchronisierung für folgende Geräte ausführen:

- Geräte, auf denen der Administrationsagent installiert ist
- Geräte mit KasperskyOS

  Stellen Sie vor dem Ausführen einer erzwungenen Synchronisierung für ein KasperskyOS-Gerät sicher, dass das Gerät im Bereich eines Verteilungspunkts enthalten ist und dass auf dem Verteilungspunkt ein Push-Server aktiviert ist.
- iOS-Geräte
- Android-Geräte

  Bevor Sie die erzwungene Synchronisierung für ein Android-Gerät ausführen, müssen Sie Firebase Cloud Messaging konfigurieren.

Synchronisation eines einzelnen Geräts

So erzwingen Sie die Synchronisierung zwischen dem Administrationsserver und dem verwalteten Gerät:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

2. Klicken Sie auf den Namen des Geräts, das mit dem Administrationsserver synchronisiert werden soll.

   Ein Eigenschaftenfenster wird geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.

3. Klicken Sie auf die Schaltfläche **Synchronisierung erzwingen**.

Die Anwendung synchronisiert das ausgewählte Gerät mit dem Administrationsserver.

Synchronisation mehrerer Geräte

So erzwingen Sie die Synchronisierung zwischen dem Administrationsserver und mehreren verwalteten Geräten:

1. Öffnen Sie die Geräteliste einer Administrationsgruppe oder einer Geräteauswahl:

   - Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**, klicken Sie auf den Pfad-Link im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte und wählen Sie anschließend die Administrationsgruppe aus, welche die zu synchronisierenden Geräte enthält.

   - Führen Sie eine Geräteauswahl durch, um die Geräteliste anzuzeigen.

2. Aktivieren Sie die Kontrollkästchen neben den Geräten, die Sie mit dem Administrationsserver synchronisieren möchten.

3. Klicken Sie über der Liste der verwalteten Geräte auf die Schaltfläche mit den 3 Punkten (...) und klicken Sie anschließend auf die Schaltfläche **Synchronisierung erzwingen**.

   Die Anwendung synchronisiert die ausgewählten Geräte mit dem Administrationsserver.

4. Prüfen Sie in der Geräteliste, dass sich die Zeit der letzten Verbindung zum Administrationsserver für die ausgewählten Geräte auf die aktuelle Zeit geändert hat. Wenn sich die Uhrzeit nicht geändert hat, aktualisieren Sie den Seiteninhalt, indem Sie auf die Schaltfläche **Aktualisieren** klicken.

Die ausgewählten Geräte wurden mit dem Administrationsserver synchronisiert.

Anzeigen des Übermittlungszeitpunktes einer Richtlinie

Nach dem Ändern einer Richtlinie für eine Kaspersky-Anwendung auf dem Administrationsserver kann der Administrator auch prüfen, ob die geänderte Richtlinie an ein bestimmtes verwaltetes Gerät übermittelt wurde. Eine Richtlinie kann während einer regulären oder einer erzwungenen Synchronisierung übermittelt werden.

Um den Zeitpunkt (Datum und Uhrzeit) anzuzeigen, zu dem eine Anwendungsrichtlinie an ein verwaltetes Gerät übermittelt wurde:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

2. Klicken Sie auf den Namen des Geräts, das mit dem Administrationsserver synchronisiert werden soll.

   Ein Eigenschaftenfenster wird geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.

3. Wählen Sie die Registerkarte **Programme** aus.

4. Wählen Sie das Programm aus, für das Sie das Datum der Richtliniensynchronisierung anzeigen möchten.

   Das Fenster mit der Programmrichtlinie wird geöffnet; dabei ist der Abschnitt **Allgemein** ausgewählt und das Datum und die Uhrzeit der Übertragung der Richtlinie werden angezeigt.

Einen Push-Server aktivieren

In Kaspersky Security Center kann ein Verteilungspunkt als Push-Server für Geräte fungieren, die über das mobile Protokoll oder über den Administrationsagenten verwaltet werden. Ein Push-Server muss beispielsweise aktiviert sein, wenn Sie die erzwungene Synchronisierung von KasperskyOS-Geräten mit dem Administrationsserver verwenden möchten. Ein Push-Server besitzt denselben Umfang verwalteter Geräte wie der Verteilungspunkt, auf dem der Push-Server aktiviert ist. Wenn Sie mehrere Verteilungspunkte derselben Administrationsgruppe zugewiesen haben, können Sie den Push-Server auf jedem der Verteilungspunkte aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

Möglicherweise möchten Sie Verteilungspunkte als Push-Server verwenden, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht. Für einige Vorgänge ist eine durchgängige Verbindung erforderlich, z. B. das Starten und Stoppen lokaler Aufgaben, das Empfangen von Statistiken für eine verwaltete Anwendung oder die Herstellung eines Tunnels. Wenn Sie einen Verteilungspunkt als Push-Server verwenden, müssen Sie weder die Option **Verbindung zum Administrationsserver nicht trennen** auf verwalteten Geräten verwenden, noch Pakete an den UDP-Port des Administrationsagenten senden.

Ein Push-Server unterstützt die Last von bis zu 50.000 gleichzeitigen Verbindungen.

So aktivieren Sie Push-Server auf einem Verteilungspunkt:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Klicken Sie auf den Namen des Verteilungspunkts, auf dem Sie den Push-Server aktivieren möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Push-Server ausführen**.

5. Geben Sie im Feld **Port des Push-Servers** die Portnummer ein. Sie können die Nummer eines beliebigen unbelegten Ports angeben.

6. Geben Sie im Feld **Remote-Host-Adresse** die IP-Adresse oder den Namen des Geräts mit dem Verteilungspunkt an.

7. Klicken Sie auf die Schaltfläche **OK**.

Der Push-Server ist auf dem ausgewählten Verteilungspunkt aktiviert.

Verwalten von Programmen von Drittanbietern auf Client-Geräten

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center für die Verwaltung von Programmen von Drittanbietern beschrieben, die auf Client-Geräten installiert sind.

Installieren von Software-Updates von Drittanbietern

Mit Kaspersky Security Center können Sie die Updates für Drittanbieter-Programme verwalten, die auf verwalteten Geräten installiert sind, und Schwachstellen in der Software von Microsoft und anderen Herstellern durch die Installation erforderlicher Updates beheben.

Kaspersky Security Center sucht mithilfe der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* nach Updates. Nach Abschluss dieser Aufgabe erhält der Administrationsserver eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Drittanbietern-Programme, die auf den Geräten installiert sind und die Sie in den Eigenschaften der Aufgabe angegeben haben. Nach Prüfen der Informationen über die verfügbaren Updates können Sie die Installation von Updates auf den Geräten durchführen.

Das Update einiger Programme von Kaspersky Security Center wird mittels Deinstallation der vorherigen Programmversion und Installation der neuen Version durchgeführt.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, das Drittanbieter-Programm zu schließen, wenn es gerade geöffnet ist.

Aus Sicherheitsgründen werden alle Updates für Drittanbieter-Programme, die Sie mittels der Funktion "Schwachstellen- und Patch-Management" installieren, automatisch von den Kaspersky-Technologien auf Schadsoftware untersucht. Die Technologien werden zur automatischen Untersuchung von Dateien verwendet und umfassen die Virensuche, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung sowie Machine-Learning-Methoden.

Kaspersky-Experten führen keine manuelle Analyse von Updates für Drittanbieter-Programme durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten in derartigen Updates weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen, noch führen sie an ihnen zusätzliche Analysen durch, die über die oben genannten hinausgehen.

Aufgaben zur Installation von Updates für Drittanbieter-Programme

Wenn Metadaten von den Programm-Updates von Drittanbietern in die Datenverwaltung heruntergeladen wurden, können Sie die folgenden Aufgaben verwenden, um die Updates auf Client-Geräten zu installieren:

- Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen*

  Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* dient dazu, Updates für Microsoft-Programme zu installieren, einschließlich der Updates, die vom Windows-Update-Dienst angeboten werden, sowie Updates für die Software anderer Hersteller. Beachten Sie, dass diese Aufgabe nur erstellt werden kann, wenn Sie eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" haben.

  Nach Abschluss dieser Aufgabe wurden die Updates automatisch auf den verwalteten Geräten installiert. Wenn Metadaten der neuen Updates in die Datenverwaltung des Administrationsservers heruntergeladen wurden, prüft Kaspersky Security Center, ob die Updates den Kriterien entsprechen, die in den Update-Regeln angegeben sind. Alle neuen Updates, welche die Kriterien erfüllen, werden beim nächsten Aufgabenstart automatisch heruntergeladen und installiert.

- Aufgabe *Windows-Updates installieren*

  Die Aufgabe *Updates von Windows Update installieren* erfordert keine Lizenz, kann aber nur für die Installation von Windows Update-Updates verwendet werden.

Nach Abschluss der Aufgabe wurden nur jene Updates installiert, die in den Aufgabeneigenschaften angegeben sind. Wenn Sie in Zukunft neue Updates installieren möchten, die in die Datenverwaltung des Administrationsservers heruntergeladen wurden, müssen Sie diese in der Liste der Updates in der vorhandenen Aufgabe hinzufügen oder eine neue Aufgabe des Typs Updates von Windows Update installieren erstellen.

Administrationsserver als WSUS-Server verwenden

Die Informationen über die verfügbaren Microsoft Windows-Updates werden vom Windows Update Center übertragen. Der Administrationsserver kann die Rolle des Windows Update-Servers übernehmen (WSUS). Um den Administrationsserver als WSUS-Server zu verwenden, erstellen Sie die Aufgabe "Windows-Updates synchronisieren" und aktivieren Sie die Option **Administrationsserver als WSUS-Server verwenden** in der Richtlinie des Administrationsagenten. Sobald die Synchronisierung der Daten mit dem Windows Update Center eingerichtet wurde, stellt der Administrationsserver im angegebenen Intervall Updates für die Windows Update-Dienste auf den Geräten bereit.

Szenario: Aktualisieren von Software von Drittanbietern

Dieser Abschnitt enthält ein Szenario für das Update von Drittanbieter-Programmen, die auf den Client-Geräten installiert sind. Als Drittanbieter-Programme gelten Anwendungen von Microsoft und von anderen Softwareherstellern. Updates für Microsoft-Programme werden vom Dienst "Windows Update" bereitgestellt.

Erforderliche Vorrausetzungen

Der Administrationsserver muss über eine Internetverbindung verfügen, um Updates anderer Drittanbietern-Programme, die keine Software von Microsoft darstellen, installieren zu können.

Standardmäßig ist für den Administrationsserver keine Internetverbindung erforderlich, um Software-Updates von Microsoft auf den verwalteten Geräten zu installieren. Beispielsweise können die verwalteten Geräte die Software-Updates von Microsoft direkt von den Microsoft Update-Servern oder von Windows Server herunterladen, wobei Microsoft Windows Server Update Services (WSUS) im Netzwerk Ihres Unternehmens bereitgestellt werden. Der Administrationsserver muss mit dem Internet verbunden sein, wenn Sie den Administrationsserver als WSUS-Server verwenden.

Schritte

Das Update von Drittanbieter-Programmen umfasst mehrere Schritte:

1. **Suche nach erforderlichen Updates**

   Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um die für die verwalteten Geräte erforderlichen Software-Updates von Drittanbietern zu suchen. Nach Abschluss dieser Aufgabe erhält Kaspersky Security Center eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Drittanbieter-Programme, die auf den Geräten installiert sind und die Sie in den Eigenschaften der Aufgabe angegeben haben.

   Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch vom Schnellstartassistenten für den Administrationsserver erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe, oder führen Sie den Schnellstartassistenten jetzt aus.

Anleitung:

- Verwaltungskonsole: Schwachstellensuche in Programmen, Zeitplan erstellen für die Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"
- Kaspersky Security Center Web Console: Aufgabe Suche nach Schwachstellen und erforderlichen Updates erstellen, Einstellungen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"

2. **Analysieren der Liste der gefundenen Updates**

   Zeigen Sie die Liste **Software-Updates** an und entscheiden Sie, welche Updates installiert werden sollen. Um detaillierte Informationen über alle Updates anzuzeigen, klicken Sie in der Liste auf den Namen des Updates. Für jedes Update in der Liste können Sie auch die Statistiken zur Update-Installation auf Client-Geräten anzeigen.

   Anleitung:

   - Verwaltungskonsole: Informationen über verfügbare Updates anzeigen
   - Kaspersky Security Center Web Console: Informationen über verfügbare Updates für Drittanbieter-Programme anzeigen

3. **Konfigurieren der Installation von Updates**

   Wenn Kaspersky Security Center die Liste der Updates für Drittanbieter-Programme erhalten hat, können Sie diese mithilfe der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* oder *Updates von Windows Update installieren* auf den Client-Geräten installieren. Erstellen Sie eine dieser Aufgaben. Sie können diese Aufgaben entweder auf der Registerkarte **Aufgaben** erstellen oder dafür die Liste **Software-Updates** verwenden.

   Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* dient dazu, Updates für Microsoft-Programme zu installieren, einschließlich der Updates, die vom Windows-Update-Dienst angeboten werden, sowie Updates für die Software anderer Hersteller. Beachten Sie, dass diese Aufgabe nur erstellt werden kann, wenn Sie eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" haben.

   Die Aufgabe *Updates von Windows Update installieren* erfordert keine Lizenz, kann aber nur für die Installation von Windows Update-Updates verwendet werden.

   Zum Installieren bestimmter Programm-Updates müssen Sie den Endbenutzer-Lizenzvertrag (EULA) für die Installationssoftware akzeptieren. Wenn Sie die EULA ablehnen, wird das Software-Update nicht installiert.

   Sie können eine Aufgabe zur Update-Installation nach Zeitplan starten. Stellen Sie im Aufgabenzeitplan sicher, dass die Aufgabe zur Update-Installation erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen wurde.

   Anleitung:

   - Verwaltungskonsole: Schwachstellen in Programmen beheben, Informationen über verfügbare Updates anzeigen
   - Kaspersky Security Center Web Console: Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen, Aufgabe "Windows-Updates installieren" erstellen, Informationen über verfügbare Updates für Drittanbieter-Programme anzeigen

4. **Planen der Aufgaben**

   Um sicherzustellen, dass die Liste der Updates immer auf dem neuesten Stand ist, planen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* so, dass sie regelmäßig automatisch ausgeführt wird. Standardmäßig ist für die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* der manuelle Start eingestellt.

   Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie festlegen, dass sie mit der gleichen Häufigkeit wie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* oder seltener ausgeführt wird. Beachten Sie beim Planen der Aufgabe *Updates von Windows Update installieren*, dass Sie jedes Mal die Liste der Updates definieren müssen, bevor Sie diese Aufgabe starten.

Stellen Sie beim Planen der Aufgaben sicher, dass die Aufgabe zum Installieren der Updates erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen ist.

5. **Genehmigen und Ablehnen von Programm-Updates (optional)**

   Falls Sie die Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellt haben, können Sie in den Aufgabeneigenschaften Regeln für die Update-Installation festlegen. Falls Sie die Aufgabe "Windows-Updates installieren" erstellt haben, überspringen Sie diesen Schritt.

   Sie können für jede Regel die zu installierenden Updates abhängig vom Update-Status definieren: *Nicht definiert*, *Genehmigt* oder *Abgelehnt*. Sie können beispielsweise eine spezielle Aufgabe für Server erstellen und für diese Aufgabe festlegen, dass nur Windows-Updates mit dem Status *Genehmigt* installiert werden dürfen. Anschließend setzen Sie für jene Updates, die Sie installieren möchten, manuell den Status *Genehmigt*. In diesem Fall werden Windows-Updates, die den Status *Nicht definiert* oder *Abgelehnt* haben, auf den in der Aufgabe angegebenen Servern nicht installiert.

   Bei einer geringen Menge an Updates ist das Verwenden des Status *Genehmigt* für die Verwaltung der Installation der Updates ist effizient. Für die Verwaltung mehrerer Updates können Sie die Regeln verwenden, die Sie in der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* konfigurieren können. Es wird empfohlen, den Status *Genehmigt* nur für die Updates zu setzen, die nicht den in den Regeln konfigurierten Kriterien entsprechen. Wenn Sie große Mengen an Updates manuell genehmigen, verringert sich die Leistungsfähigkeit des Administrationsservers, was zu einer Überlastung des Servers führen kann.

   Standardmäßig besitzen heruntergeladene Software-Updates den Status *Nicht definiert*. Sie können den Status in der Liste **Software-Updates** auf *Genehmigt* oder *Abgelehnt* ändern (**Vorgänge** → **Patch-Management** → **Software-Updates**).

   Anleitung:

   - Verwaltungskonsole: Genehmigen und Ablehnen von Software-Updates
   - Kaspersky Security Center Web Console: Genehmigen und Ablehnen der Updates von Drittanbieter-Programmen

6. **Administrationsserver anpassen, damit er als Server für Windows Server Update Services (WSUS) funktioniert (optional)**

   Windows-Updates werden standardmäßig von den Microsoft-Servern auf die verwalteten Geräte heruntergeladen. Sie können diese Einstellung ändern, um den Administrationsserver als WSUS-Server zu verwenden. In diesem Fall synchronisiert der Administrationsserver die Update-Daten in festgelegten Zeitabständen mit Windows Update und stellt die Updates für Windows Update im zentralisierten Modus auf den Netzwerkgeräten bereit.

   Um den Administrationsserver als WSUS-Server zu verwenden, erstellen Sie die Aufgabe "Windows-Updates synchronisieren" und aktivieren Sie das Kontrollkästchen **Administrationsserver als WSUS-Server verwenden** in der Richtlinie des Administrationsagenten.

   Anleitung:

   - Verwaltungskonsole: Windows-Updates mit dem Administrationsserver synchronisieren, Windows-Updates in der Richtlinie des Administrationsagenten anpassen
   - Kaspersky Security Center Web Console: Erstellen der Aufgabe "Windows-Updates synchronisieren"

7. **Ausführen einer Aufgabe zum Installieren von Updates**

   Starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Updates von Windows Update installieren*. Wenn Sie diese Aufgaben starten, werden die Updates heruntergeladen und auf den verwalteten Geräten installiert. Stellen Sie nach Abschluss der Aufgabe sicher, dass sie in der Liste den Status *Erfolgreich abgeschlossen* hat.

8. **Erstellen des Berichts über die Installationsergebnisse der Updates für Drittanbieter-Programme (optional)**

Um eine detaillierte Statistik über die Update-Installation anzuzeigen, erstellen Sie den **Bericht über die Installationsergebnisse der Updates von Drittanbieterprogrammen**.

Anleitung:

- Verwaltungskonsole: Bericht erstellen und anzeigen
- Kaspersky Security Center Web Console: Erzeugen und Anzeigen von Berichten

Ergebnisse

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt und angepasst haben, werden die Updates automatisch auf den verwalteten Geräten installiert. Wenn neue Updates in die Datenverwaltung des Administrationsservers heruntergeladen wurden, prüft Kaspersky Security Center, ob die Updates den Kriterien aus den Update-Regeln entsprechen. Alle neuen Updates, welche die Kriterien erfüllen, werden beim nächsten Aufgabenstart automatisch installiert.

Wenn Sie die Aufgabe *Updates von Windows Update installieren* erstellt haben, werden nur die in den Aufgabeneigenschaften *Updates von Windows Update installieren* angegeben Updates installiert. Wenn Sie in Zukunft neue Updates installieren möchten, die in die Datenverwaltung des Administrationsservers heruntergeladen wurden, müssen Sie diese in der Liste der Updates in der vorhandenen Aufgabe hinzufügen oder eine neue Aufgabe des Typs *Updates von Windows Update installieren* erstellen.

Installieren von Software-Updates von Drittanbietern

Sie können Updates für Drittanbieter-Programme auf verwalteten Geräten installieren, indem Sie eine der folgenden Aufgaben erstellen und ausführen:

- *Erforderliche Updates installieren und Schwachstellen schließen*

  Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* kann nur erstellt werden, wenn Sie eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" haben. Sie können die Aufgabe sowohl für die Installation von durch Microsoft bereitgestellte Updates von Windows Update, also auch für Programm-Updates von anderen Hersteller verwenden.

- *Windows-Updates installieren*

  Um nur Updates von Windows Update zu installieren, können Sie die Aufgabe *Windows-Updates installieren* verwenden.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, das Drittanbieter-Programm zu schließen, wenn es gerade geöffnet ist.

Optional können Sie eine Aufgabe erstellen, um die erforderlichen Updates auf folgende Weise zu installieren:

- Indem Sie die Update-Liste öffnen und angeben, welche Updates installiert werden sollen.

  Als Ergebnis wird eine neue Aufgabe zum Installieren der ausgewählten Updates erstellt. Optional können Sie die ausgewählten Updates zu einer vorhandenen Aufgabe hinzufügen.

- Indem Sie den Assistenten für die Installation von Updates ausführen.

Der Update-Installationsassistent ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Der Assistent vereinfacht die Erstellung und Konfiguration einer Aufgabe zum Konfigurieren der Update-Installation und ermöglicht es Ihnen, die Erstellung redundanter Aufgaben zu vermeiden, die dieselben zu installierenden Updates enthalten.

Installieren von Updates für Drittanbieter-Programme mithilfe der Update-Liste

Um Updates für Drittanbieter-Programme mithilfe der Liste der Updates zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie eine der Listen mit Updates:

   - Um die allgemeine Update-Liste zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Software-Updates**.
   - Um die Liste mit Updates für ein verwaltetes Gerät zu öffnen, wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte** → <Gerätename> → **Erweitert** → **Verfügbare Updates**.
   - Um die Liste mit Updates für ein bestimmtes Programm zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry** → <Programmname> → **Verfügbare Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

2. Aktivieren Sie die Kontrollkästchen neben den Updates, die Sie installieren möchten.

3. Klicken Sie auf die Schaltfläche **Updates installieren**.

   Zum Installieren bestimmter Software-Updates müssen Sie den Endbenutzer-Lizenzvertrag (EULA) akzeptieren. Wenn Sie die EULA ablehnen, wird das Programm-Update nicht installiert.

4. Wählen Sie eine der folgenden Varianten aus:

   - **Neue Aufgabe**

     Der Assistent für das Erstellen einer Aufgabe wird gestartet. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management verfügen, wird die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* vorausgewählt. Wenn Sie nicht über die Lizenz verfügen, wird die Aufgabe *Windows-Updates installieren* vorausgewählt. Folgen Sie den Schritten des Assistenten, um die Erstellung der Aufgabe abzuschließen.

   - **Update installieren (Regel zur angegebenen Aufgabe hinzufügen)**

     Wählen Sie eine Aufgabe, der Sie die ausgewählten Updates hinzufügen möchten. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management Lizenz für Schwachstellen- und Patch-Management verfügen, wählen Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* aus. Eine neue Regel für die Installation der gewählten Updates wird der ausgewählten Aufgabe automatisch hinzugefügt. Wenn Sie nicht über die Lizenz verfügen, wählen Sie die Aufgabe *Windows-Updates installieren* aus. Die ausgewählten Updates werden den Aufgabeneigenschaften hinzugefügt.

Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wenn Sie sich entschieden haben, eine Aufgabe zu erstellen, so wird diese Aufgabe in der Aufgabenliste unter **Assets (Geräte)** → **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Aufgaben zu einer vorhandenen Aufgabe hinzuzufügen, werden die Updates in den Aufgabeneigenschaften gespeichert.

Um Updates für Drittanbieter-Programme zu installieren, starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Windows-Updates installieren*. Sie können jede dieser Aufgaben entweder manuell starten oder in den Eigenschaften der entsprechenden Aufgabe einen Zeitplan festlegen. Stellen Sie im Aufgabenzeitplan sicher, dass die Aufgabe zur Update-Installation erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen wurde.

Installieren von Updates für Drittanbieter-Programme mithilfe des Assistenten für die Installation von Updates

Der Assistent für die Installation von Updates ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

So erstellen Sie eine Aufgabe zur Installation der Updates für Drittanbieter-Programme mithilfe des Assistenten für die Installation von Updates:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Software-Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

2. Aktivieren Sie das Kontrollkästchen neben dem Update, das Sie installieren möchten.

3. Klicken Sie auf **Assistent zur Installation von Updates starten**.

   Der Assistent für die Installation von Updates wird gestartet. Die Seite **Wählen Sie die Aufgabe zur Installation von Updates aus** enthält die Liste aller vorhandenen Aufgaben der folgenden Arten an:

   - *Erforderliche Updates installieren und Schwachstellen schließen*
   - *Windows-Updates installieren*
   - *Schwachstellen schließen*

   Sie können die beiden letzteren Aufgabentypen nicht anpassen, um neue Updates zu installieren. Um neue Updates zu installieren, können Sie nur Aufgaben des Typs *Erforderliche Updates installieren und Schwachstellen schließen* verwenden.

4. Wenn der Assistent nur die Aufgaben anzeigen soll, mit denen das von Ihnen ausgewählte Update installiert werden soll, aktivieren Sie die Option **Nur Aufgaben anzeigen, die das Update installieren**.

5. Wählen Sie, was Sie tun möchten:

- Um eine Aufgabe zu starten, aktivieren Sie das Kontrollkästchen neben dem Aufgabennamen und klicken auf die Schaltfläche **Starten**.
- So fügen Sie einer vorhandenen Aufgabe eine neue Regel hinzu:

  a. Aktivieren Sie das Kontrollkästchen neben dem Aufgabennamen und klicken Sie auf die Schaltfläche **Regel hinzufügen**.

  b. Konfigurieren Sie auf der sich öffnenden Seite die neue Regel:

  - **Regel für die Installation von Updates dieser Ereigniskategorie**

    Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

    Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

    Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

    Diese Option ist standardmäßig deaktiviert.

  - **Regel für die Installation von Updates dieser Ereigniskategorie nach MSRC**

    Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

    Wenn diese Option aktiviert ist (nur für Windows Update verfügbar), schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

    Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

    Diese Option ist standardmäßig deaktiviert.

  - **Regel für die Installation von Updates dieses Herstellers**

    Diese Option ist nur für Updates von Drittanbieter-Anwendungen verfügbar. Kaspersky Security Center installiert nur die Updates, die sich auf Programme beziehen, die vom selben Anbieter wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Anbieter werden nicht installiert.

    Diese Option ist standardmäßig deaktiviert.

  - **Regel für die Installation von Updates vom Typ**
  - **Regel für die Installation des ausgewählten Updates**
  - **Ausgewählte Updates bestätigen**

Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

Diese Option ist standardmäßig deaktiviert.

- **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

  Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

  Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

  Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

  Diese Option ist standardmäßig aktiviert.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

- So erstellen Sie eine Aufgabe:

  a. Klicken Sie auf **Neue Aufgabe**.

  b. Konfigurieren Sie auf der sich öffnenden Seite die neue Regel:

  - **Regel für die Installation von Updates dieser Ereigniskategorie**

    Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

    Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

    Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

    Diese Option ist standardmäßig deaktiviert.

  - **Regel für die Installation von Updates dieser Ereigniskategorie nach MSRC**

    Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

    Wenn diese Option aktiviert ist (nur für Windows Update verfügbar), schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

    Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

Diese Option ist standardmäßig deaktiviert.

- **Regel für die Installation von Updates dieses Herstellers**

  Diese Option ist nur für Updates von Drittanbieter-Anwendungen verfügbar. Kaspersky Security Center installiert nur die Updates, die sich auf Programme beziehen, die vom selben Anbieter wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Anbieter werden nicht installiert.

  Diese Option ist standardmäßig deaktiviert.

- **Regel für die Installation von Updates vom Typ**

- **Regel für die Installation des ausgewählten Updates**

- **Ausgewählte Updates bestätigen**

  Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

- **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

  Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

  Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

  Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

  Diese Option ist standardmäßig aktiviert.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Wenn Sie sich entschieden haben, eine Aufgabe zu starten, können Sie den Assistenten schließen. Die Aufgabe wird im Hintergrundmodus durchgeführt. Es sind keine weiteren Aktionen erforderlich.

Wenn Sie sich entschieden haben, die Regel zu einer vorhandenen Aufgabe hinzuzufügen, wird das Fenster mit den Aufgabeneigenschaften geöffnet. Die neue Regel wurde den Aufgabeneigenschaften bereits hinzugefügt. Sie können die Regel oder andere Aufgabeneigenschaften anzeigen und anpassen. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wenn Sie eine Aufgabe erstellen möchten, fahren Sie im Assistenten für das Erstellen einer Aufgabe mit der Erstellung der Aufgabe fort. Die neue Regel, die Sie im Assistenten zur Installation von Updates hinzugefügt haben, wird im Assistenten für das Erstellen einer Aufgabe angezeigt. Wenn Sie den Assistenten abgeschlossen haben, wird die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* zur Aufgabenliste hinzugefügt.

Erstellen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"

Über die Aufgabe Suche nach Schwachstellen und erforderlichen Updates erhält Kaspersky Security Center eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Drittanbieter-Programme, die auf den verwalteten Geräten installiert ist.

Die Aufgabe Suche nach Schwachstellen und erforderlichen Updates wird automatisch erstellt, wenn der Schnellstartassistent ausgeführt wird. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe manuell.

So erstellen Sie die Aufgabe Suche nach Schwachstellen und erforderlichen Updates:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Suche nach Schwachstellen und erforderlichen Updates**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.
6. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.
7. Klicken Sie auf **Erstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste angezeigt.
8. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
9. Geben Sie im Fenster mit den Aufgabeneigenschaften die allgemeinen Aufgabeneinstellungen an.
10. Geben Sie auf der Registerkarte **Programmeinstellungen** die folgenden Einstellungen an:

    - **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

      Wenn Kaspersky Security Center nach Schwachstellen und Updates sucht, verwendet das Programm die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

      Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und Updates für Drittanbieter-Apps haben.

      Diese Option ist standardmäßig aktiviert.

      Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Mit dem Update-Server verbinden, um Daten zu aktualisieren**

  Der Windows-Update-Agent auf einem verwalteten Gerät stellt eine Verbindung zur Quelle für Microsoft-Updates her. Die folgenden Server können als Quelle für Microsoft-Updates dienen:

  - Kaspersky Security Center Administrationsserver (siehe Einstellungen der Richtlinie des Administrationsagenten)
  - Windows Server mit Microsoft Windows Server Update Services (WSUS), das in Ihrem Unternehmensnetzwerk bereitgestellt wurde
  - Microsoft-Update-Server

  Wenn diese Option aktiviert ist, stellt der Windows-Update-Agent auf einem verwalteten Gerät eine Verbindung zur Quelle für Microsoft-Updates her, um die Informationen über geeignete Microsoft-Windows-Updates zu aktualisieren.

  Wenn diese Option deaktiviert ist, verwendet der Windows-Update-Agent auf einem verwalteten Gerät die Informationen über geeignete Microsoft Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden.

  Das Herstellen einer Verbindung zur Quelle für Microsoft-Updates kann ressourcenaufwendig sein. Sie können diese Option deaktivieren, wenn Sie in einer anderen Aufgabe oder in den Eigenschaften der Administrationsagenten-Richtlinie im Abschnitt **Software-Updates und Schwachstellen** eine regelmäßige Verbindung zu dieser Update-Quelle festgelegt haben. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um eine Überlastung des Servers zu vermeiden.

  Diese Option ist standardmäßig aktiviert.

  Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, die in den Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

  - Der Windows-Update-Agent auf einem verwalteten Gerät stellt nur unter den folgenden Bedingungen eine Verbindung zum Update-Server her, um Updates zu erhalten: Die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** in den Eigenschaften der Aufgabe zum *Suche nach Schwachstellen und erforderlichen Updates* ist aktiviert und die Option **Modus für die Suche nach Windows-Updates** steht in den Einstellungen der Administrationsagent-Richtlinie auf **Aktiv**.
  - Wenn Sie den Administrationsagenten nicht benötigen, um während der Ausführung der Aufgabe *Untersuchung auf Schwachstellen* eine Verbindung zur Microsoft Windows-Update-Quelle herzustellen und Updates herunterzuladen, können Sie die Option **Modus für die Suche nach Windows-Updates** auf **Offline** setzen, wobei die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert bleiben muss. Auf diese Weise können Sie Ressourcen sparen und zuvor abgerufene Windows-Updates verwenden, um nach Schwachstellen zu suchen. Sie können den passiven Modus verwenden, wenn Sie das Abrufen von Microsoft Windows-Updates auf eine andere Art konfigurieren. Wenn das Abrufen von Microsoft Windows-Updates jedoch nicht auf eine andere Art konfiguriert ist, setzen Sie die Option **Modus für die Suche nach Windows-Updates** nicht auf **Offline**, da in diesem Fall keine Informationen über Updates abgerufen werden.
  - Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert), wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** gesetzt ist, fragt Kaspersky Security Center keine Informationen über Updates ab.

- **Nach Schwachstellen und Updates von Drittherstellern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Security Center in der Windows-Registrierung und den unter Geben Sie Pfade für eine zusätzliche Suche nach Programmen im Dateisystem an **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für fremde Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

  Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps haben.

  Diese Option ist standardmäßig aktiviert.

- **Pfade für die erweiterte Suche nach Anwendungen im Dateisystem angeben**

  Die Ordner, in denen Kaspersky Security Center nach Drittanbieter-Apps sucht, für die ein Schließen von Schwachstellen und eine Update-Installation erforderlich ist. Sie können Systemvariable verwenden.

  Legen Sie die Ordner fest, in denen Programme installiert sind. Standardmäßig enthält die Liste die Systemordner, in denen die meisten Programme installiert sind.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

11. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.

Wenn die Aufgabenergebnisse eine Warnung des Fehlers 0x80240033 "Windows Update Agent error 80240033 ("Lizenzbedingungen konnten nicht heruntergeladen werden.")" enthalten, können Sie dieses

Problem über die Windows-Registrierung beheben.

Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates

Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch erstellt, wenn der Schnellstartassistent ausgeführt wird. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe manuell.

Neben den allgemeinen Aufgabeneinstellungen können Sie die folgenden Einstellungen vornehmen, wenn Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erstellen oder wenn Sie die Eigenschaften der erstellten Aufgabe später konfigurieren:

- **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

  Wenn Kaspersky Security Center nach Schwachstellen und Updates sucht, verwendet das Programm die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

  Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und Updates für Drittanbieter-Apps haben.

  Diese Option ist standardmäßig aktiviert.

  Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Mit dem Update-Server verbinden, um Daten zu aktualisieren**

  Der Windows-Update-Agent auf einem verwalteten Gerät stellt eine Verbindung zur Quelle für Microsoft-Updates her. Die folgenden Server können als Quelle für Microsoft-Updates dienen:

  - Kaspersky Security Center Administrationsserver (siehe Einstellungen der Richtlinie des Administrationsagenten)
  - Windows Server mit Microsoft Windows Server Update Services (WSUS), das in Ihrem Unternehmensnetzwerk bereitgestellt wurde
  - Microsoft-Update-Server

  Wenn diese Option aktiviert ist, stellt der Windows-Update-Agent auf einem verwalteten Gerät eine Verbindung zur Quelle für Microsoft-Updates her, um die Informationen über geeignete Microsoft-Windows-Updates zu aktualisieren.

  Wenn diese Option deaktiviert ist, verwendet der Windows-Update-Agent auf einem verwalteten Gerät die Informationen über geeignete Microsoft Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden.

  Das Herstellen einer Verbindung zur Quelle für Microsoft-Updates kann ressourcenaufwendig sein. Sie können diese Option deaktivieren, wenn Sie in einer anderen Aufgabe oder in den Eigenschaften der Administrationsagenten-Richtlinie im Abschnitt **Software-Updates und Schwachstellen** eine regelmäßige Verbindung zu dieser Update-Quelle festgelegt haben. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um eine Überlastung des Servers zu vermeiden.

  Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, die in den Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Der Windows-Update-Agent auf einem verwalteten Gerät stellt nur unter den folgenden Bedingungen eine Verbindung zum Update-Server her, um Updates zu erhalten: Die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** in den Eigenschaften der Aufgabe zum *Suche nach Schwachstellen und erforderlichen Updates* ist aktiviert und die Option **Modus für die Suche nach Windows-Updates** steht in den Einstellungen der Administrationsagent-Richtlinie auf **Aktiv**.

- Wenn Sie den Administrationsagenten nicht benötigen, um während der Ausführung der Aufgabe *Untersuchung auf Schwachstellen* eine Verbindung zur Microsoft Windows-Update-Quelle herzustellen und Updates herunterzuladen, können Sie die Option **Modus für die Suche nach Windows-Updates** auf **Offline** setzen, wobei die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert bleiben muss. Auf diese Weise können Sie Ressourcen sparen und zuvor abgerufene Windows-Updates verwenden, um nach Schwachstellen zu suchen. Sie können den passiven Modus verwenden, wenn Sie das Abrufen von Microsoft Windows-Updates auf eine andere Art konfigurieren. Wenn das Abrufen von Microsoft Windows-Updates jedoch nicht auf eine andere Art konfiguriert ist, setzen Sie die Option **Modus für die Suche nach Windows-Updates** nicht auf **Offline**, da in diesem Fall keine Informationen über Updates abgerufen werden.

- Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert), wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** gesetzt ist, fragt Kaspersky Security Center keine Informationen über Updates ab.

- **Nach Schwachstellen und Updates von Drittherstellern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Security Center in der Windows-Registrierung und den unter Geben Sie Pfade für eine zusätzliche Suche nach Programmen im Dateisystem an **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für fremde Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

  Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps haben.

  Diese Option ist standardmäßig aktiviert.

- **Pfade für die erweiterte Suche nach Anwendungen im Dateisystem angeben**

  Die Ordner, in denen Kaspersky Security Center nach Drittanbieter-Apps sucht, für die ein Schließen von Schwachstellen und eine Update-Installation erforderlich ist. Sie können Systemvariable verwenden.

  Legen Sie die Ordner fest, in denen Programme installiert sind. Standardmäßig enthält die Liste die Systemordner, in denen die meisten Programme installiert sind.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, falls die Informationen in von Ihnen gesendeten Dateien der erweiterten Diagnose nicht ausreichen, um das Problem zu beheben.

Tipps für den Aufgabenzeitplan

Stellen Sie bei der Planung der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* sicher, dass die beiden Optionen **Übersprungene Aufgaben starten** und **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert sind.

Standardmäßig ist für die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* der manuelle Start eingestellt. Wenn zu diesem Zeitpunkt alle Geräte aufgrund der Regeln und Vorschriften des Unternehmens deaktiviert sind, wird die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ausgeführt, nachdem die Geräte wieder eingeschaltet werden (also am Morgen des folgenden Tages). Ein solches Verhalten kann unerwünscht sein, da die Untersuchung auf Schwachstellen eine erhöhte Belastung des Prozessors und des Laufwerkssubsystems verursachen kann. Für einen optimalen Aufgabenzeitplan sollten die im Unternehmen geltenden Regeln und Vorschriften berücksichtigt werden.

Erstellen der Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen"

> Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Drittanbieter-Programmen, einschließlich Microsoft, die auf den verwalteten Geräten installiert ist, zu aktualisieren und zu beheben. Mit dieser Aufgabe können Sie mehrere Updates installieren und mehrere Schwachstellen nach bestimmten Regeln beheben.

Sie haben eine der folgenden Möglichkeiten, um mithilfe der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* Updates zu installieren oder Schwachstellen zu schließen:

- Führen Sie den Assistenten für die Installation von Updates oder den Assistenten für das Schließen von Schwachstellen aus.
- Erstellen einer Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Fügen Sie eine Regel für die Update-Installation zu einer bestehenden Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* hinzu.

So erstellen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Erforderliche Updates installieren und Schwachstellen schließen**.

   Wenn die Aufgabe nicht angezeigt wird, prüfen Sie, ob Ihr Benutzerkonto über die Berechtigungen **Lesen**, **Ändern** und **Ausführen** für den Funktionsbereich **Systemverwaltung**: **Schwachstellen- und Patch-Management** verfügt. Sie könne die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen"* ohne diese Zugriffsrechte nicht erstellen und konfigurieren.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.
6. Geben Sie die Regeln für die Update-Installation und dann die folgenden Einstellungen an:

   - **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen**

     Ist diese Option aktiviert, so werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Andernfalls werden Updates nach einem Zeitplan installiert.

     Verwenden Sie diese Option, wenn die Installation von Updates die Geräteleistung beeinträchtigen könnte.

     Diese Option ist standardmäßig deaktiviert.

   - **Erforderliche allgemeine Systemkomponenten installieren**

     Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

     Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

     Diese Option ist standardmäßig deaktiviert.

   - **Installation einer neuen Programmversion beim Update zulassen**

     Ist diese Option aktiviert, so werden Updates erlaubt, wenn sie zur Installation einer neuen Version einer Softwareanwendung führen.

     Wenn diese Option deaktiviert ist, wird die Software nicht aktualisiert. Sie können dann neue Versionen der Software manuell oder über eine andere Aufgabe installieren. Sie können diese Option beispielsweise verwenden, wenn die Infrastruktur Ihres Unternehmens nicht von einer neuen Softwareversion unterstützt wird oder wenn Sie ein Update in einer Testinfrastruktur überprüfen möchten.

     Diese Option ist standardmäßig aktiviert.

     > Aktualisieren einer Anwendung kann zu Fehlern bei abhängigen Anwendungen führen, die auf Client-Geräten installiert sind.

- **Updates auf das Gerät herunterladen, ohne sie zu installieren**

  Wenn diese Option aktiviert ist, lädt die Anwendung Updates auf das Gerät herunter, installiert sie jedoch nicht automatisch. Sie können die heruntergeladenen Updates dann manuell installieren.

  Microsoft-Updates werden in den Windows-Systemspeicher heruntergeladen. Updates für Drittanbieter-Anwendungen (Anwendungen, die von den Software-Herstellern Kaspersky oder Microsoft stammen) werden in den Ordner heruntergeladen, der im Feld **Updates herunterladen nach** angegeben ist.

  Wenn diese Option deaktiviert ist, werden die Updates automatisch auf dem Gerät installiert.

  Diese Option ist standardmäßig deaktiviert.

- **Updates herunterladen nach**

  Dieser Ordner wird verwendet, um Updates für Drittanbieter-Anwendungen (Anwendungen, die nicht von den Software-Herstellern Kaspersky oder Microsoft stammen) herunterzuladen.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

7. Geben Sie Neustart-Einstellungen des Betriebssystems an:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

- **Aufforderung regelmäßig wiederholen nach (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Wartezeit vor dem erzwungenen Schließen von Programmen in gesperrten Sitzungen (Min.)**

  Programme werden zwangsweise geschlossen, wenn das Benutzergerät gesperrt wird (automatisch nach einer bestimmten Inaktivitätsdauer oder manuell).

  Wenn diese Option aktiviert ist, werden Programme auf einem gesperrten Gerät nach Ablauf der im Eingabefeld angegebenen Zeitspanne automatisch geschlossen.

  Wenn diese Option deaktiviert ist, werden Programme auf einem gesperrten Gerät nicht geschlossen.

  Diese Option ist standardmäßig deaktiviert.

8. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

10. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

11. Geben Sie im Fenster mit den Aufgabeneigenschaften die passenden allgemeinen Aufgabeneinstellungen an.

12. Klicken Sie auf die Schaltfläche **Speichern**.

    Die Aufgabe wird erstellt und konfiguriert.

Wenn die Aufgabenergebnisse eine Warnung des Fehlers 0x80240033 "Windows Update Agent error 80240033 ("Lizenzbedingungen konnten nicht heruntergeladen werden.")" enthalten, können Sie dieses Problem über die Windows-Registrierung beheben.

Hinzufügen einer Regel für die Installation von Updates

Diese Funktion ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Beim Installieren von Programm-Updates oder beim Schließen von Schwachstellen in Programmen mittels der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* müssen Sie Regeln für die Update-Installation angeben. Diese Regeln bestimmen, welche Updates installiert und welche Schwachstellen geschlossen werden.

Die genauen Einstellungen hängen davon ab, ob Sie eine Regel für alle Updates, für Windows Update-Updates oder für Updates von Drittanbieter-Programmen (Programme von anderen Softwareherstellern als Kaspersky und Microsoft) hinzufügen. Beim Hinzufügen einer Regel für Windows Update-Updates oder Updates von Drittanbieter-Programmen können Sie bestimme Programme und Programmversionen auswählen, für die Sie Updates installieren möchten. Beim Hinzufügen einer Regel für alle Updates können Sie bestimmte Updates, die Sie installieren möchten, und Schwachstellen, die Sie mittels Installation von Updates schließen möchten, auswählen.

Sie können eine Regel für die Update-Installation auf folgende Arten hinzufügen:

- Durch Hinzufügen einer Regel beim Erstellen einer neuen Aufgabe des Typs Erforderliche Updates installieren und Schwachstellen schließen.
- Durch Hinzufügen einer Regel auf der Registerkarte **Programmeinstellungen** im Eigenschaftenfenster einer vorhandenen Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Durch Ausführen des Assistenten für die Installation von Updates oder des Assistenten für das Schließen von Schwachstellen.

Um eine neue Regel für alle Updates hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

2. Wählen Sie auf der Seite **Regeltyp** den Typ **Regel für alle Updates** aus.

3. Verwenden Sie auf der Seite **Allgemeine Kriterien** die Dropdown-Listen, um die folgenden Einstellungen festzulegen:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.
     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.
     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

- **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

  Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

  Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

  Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

  Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Updates** die Updates aus, die installiert werden sollen:

   - **Alle relevanten Updates installieren**

     Installieren Sie alle Programm-Updates, von denen die im Assistenten auf der Seite **Allgemeine Kriterien** aufgeführten Kriterien erfüllt werden. Standardmäßig ausgewählt.

   - **Nur Updates aus der Liste installieren**

     Es werden nur Programm-Updates installiert, die Sie in der Liste manuell auswählen. Diese Liste enthält alle verfügbaren Programm-Updates.

     Sie können beispielsweise in den folgenden Fällen bestimmte Updates auswählen: um deren Installation in einer Testumgebung zu überprüfen, um nur kritische Programme zu aktualisieren oder um nur bestimmte Programme zu aktualisieren.

     - **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

       Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

       Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

       Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

       Diese Option ist standardmäßig aktiviert.

5. Wählen Sie auf der Seite **Schwachstellen** jene Schwachstellen aus, die durch die Installation der ausgewählten Updates geschlossen werden:

   - **Alle Schwachstellen schließen, die den übrigen Kriterien entsprechen**

     Beheben Sie alle Schwachstellen, welche die Kriterien auf der Seite **Allgemeine Kriterien** des Assistenten erfüllen. Standardmäßig ausgewählt.

   - **Nur Schwachstellen aus der Liste schließen**

     Es werden nur Schwachstellen geschlossen, die Sie manuell aus der Liste auswählen. Diese Liste enthält alle gefundenen Schwachstellen.

Sie können beispielsweise in den folgenden Fällen bestimmte Schwachstellen auswählen: um deren Schließen in einer Testumgebung zu überprüfen, um Schwachstellen nur in kritischen Apps zu schließen oder um Schwachstellen nur in bestimmten Programmen zu aktualisieren.

6. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie hinzufügen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem dem Abschließen des Assistenten für das Erstellen einer Regel wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgabe oder in den Aufgabeneigenschaften angezeigt.

Um eine neue Regel für Windows Update-Updates hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

2. Wählen Sie auf der Seite **Regeltyp** den Typ **Regel für Windows-Updates** aus.

3. Passen Sie auf der Seite **Allgemeine Kriterien** die folgenden Einstellungen an:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.
     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.
     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

   - **Schwachstellen schließen, deren MSRC-Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Anwendungen** die Programme und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Wählen Sie auf der Seite **Update-Kategorien** die Kategorien der Updates aus, die installiert werden sollen. Diese Kategorien entsprechen den Kategorien im Microsoft-Update-Katalog. Standardmäßig sind alle Kategorien ausgewählt.

6. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie hinzufügen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem dem Abschließen des Assistenten für das Erstellen einer Regel wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgabe oder in den Aufgabeneigenschaften angezeigt.

Um eine neue Regel für Updates von Drittanbieter-Programmen hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

2. Wählen Sie auf der Seite **Regeltyp** den Typ **Regel für Updates von Drittherstellern** aus.

3. Passen Sie auf der Seite **Allgemeine Kriterien** die folgenden Einstellungen an:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.

     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.

     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Anwendungen** die Programme und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie hinzufügen. Sie können diesen Namen später im Abschnitt Einstellungen des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem dem Abschließen des Assistenten für das Erstellen einer Regel wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgabe oder in den Aufgabeneigenschaften angezeigt.

Erstellen der Aufgabe "Windows-Updates installieren"

Mit der Aufgabe *Windows-Updates installieren* können Sie Programm-Updates installieren, die vom Windows Update-Dienst auf den verwalteten Geräten bereitgestellt werden.

Wenn Sie nicht über die Lizenz für Schwachstellen- und Patch-Management verfügen, können Sie keine neuen Aufgaben des Typs *Windows-Updates installieren* erstellen. Um neue Updates zu installieren, können Sie diese zu einer bestehenden *Windows-Updates installieren*-Aufgabe hinzufügen. Wir empfehlen die Verwendung der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* statt der Aufgabe *Windows-Updates installieren*. Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ermöglicht es Ihnen, mehrere Updates zu installieren und mehrere Schwachstellen automatisch gemäß den von Ihnen definierten Regeln zu schließen. Darüber hinaus ermöglicht Ihnen diese Aufgabe, Updates von anderen Softwareanbietern als Microsoft zu installieren.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, ein momentan geöffnetes Drittanbieter-Programm zu schließen.

Um die Aufgabe "Windows-Updates installieren" zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Windows-Updates installieren**.

4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen.

   Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.

6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Die Liste der Updates wird geöffnet.

7. Wählen Sie die Windows-Updates aus, die Sie installieren möchten, und klicken Sie dann auf **OK**.

8. Geben Sie Neustart-Einstellungen des Betriebssystems an:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

- **Aufforderung regelmäßig wiederholen nach (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

9. Legen Sie die Benutzerkonto-Einstellungen fest:

   - **Standardbenutzerkonto**

     Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

     Diese Variante ist standardmäßig ausgewählt.

   - **Benutzerkonto festlegen**

     Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

   - **Benutzerkonto**

     Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

   - **Kennwort**

     Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

10. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

11. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

12. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

13. Geben Sie im Fenster mit den Aufgabeneigenschaften die passenden allgemeinen Aufgabeneinstellungen an.

14. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.

Anzeigen von Informationen zu verfügbaren Updates von Drittanbieter-Programmen

Sie können die Liste der verfügbaren Updates für Software von Drittanbietern, einschließlich Microsoft, die auf Client-Geräten installiert ist, anzeigen.

Um eine Liste der verfügbaren Updates für die auf den Client-Geräten installierten Programme von Drittanbietern anzuzeigen, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Software-Updates**.

Eine Liste verfügbarer Updates wird geöffnet.

Sie können einen Filter angeben, um die Liste der Software-Updates anzuzeigen. Klicken Sie auf das **Filter**-Symbol () oben rechts in der Liste der Programm-Updates, um den Filter anzupassen. Sie können auch einen der voreingestellten Filter aus der Dropdown-Liste **Vordefinierte Filter** oberhalb der Liste mit Schwachstellen in Programmen auswählen.

Um sich die Eigenschaften eines Updates anzusehen:

1. Klicken Sie auf den Namen des gewünschten Programm-Updates.
2. Das Fenster mit den Update-Eigenschaften wird geöffnet. Es enthält die folgenden Registerkarten:

   - **Allgemein**

     Die Registerkarte enthält allgemeine Informationen über das ausgewählte Update:

     - Genehmigungsstatus des Updates (Kann manuell durch Auswahl eines neuen Status in der Dropdown-Liste geändert werden)
     - Kategorie des Windows Server Update-Dienstes (WSUS), der das Update zugeordnet ist
     - Datum und Uhrzeit der Registrierung des Updates
     - Datum und Uhrzeit der Erstellung des Updates
     - Ereigniskategorie des Updates
     - Installationsvoraussetzungen, die für das Update gelten
     - Programmfamilie, zu der das Update gehört
     - Programm, zu dem das Update gehört
     - Revisionsnummer des Updates

   - **Attribute**

     Diese Registerkarte enthält eine Auswahl von Eigenschaften des Updates, die Sie verwenden können, um weitere Informationen über das Update zu erhalten. Die Auswahl unterscheidet sich je nachdem, ob es sich um ein Update von Microsoft oder von einem Drittanbieter handelt.

     Für ein Microsoft-Update enthält die Registerkarte die folgenden Informationen:

     - Ereigniskategorie des Updates, gemäß Microsoft Security Response Center (MSRC)
     - Link zu dem Artikel in der Microsoft Knowledge Base, in dem das Update beschrieben ist
     - Link zu dem Artikel in dem Microsoft-Sicherheitsbulletin, in dem das Update beschrieben ist
     - Update-Identifikator (ID)

     Für ein Drittanbieter-Update enthält die Registerkarte die folgenden Informationen:

     - Ob das Update ein Patch oder ein vollständiges Programmpaket ist
     - Lokalisierungssprache des Updates

- Ob das Update automatisch oder manuell installiert wird
- Ob das Update nach der Genehmigung widerrufen wurde
- Download-Link für das Update

- **Geräte**

  Diese Registerkarte enthält eine Liste mit den Geräten, auf denen das ausgewählte Update installiert wurde.

- **Zu schließende Schwachstellen**

  Diese Registerkarte enthält eine Liste der Schwachstellen, die das ausgewählte Update schließen kann.

- **Überschneidungen von Updates**

  Diese Registerkarte enthält Überschneidungen von verschiedenen, für dasselbe Programm veröffentlichten Updates. Das heißt, ob das Update andere Updates ersetzen kann oder ob es selbst durch andere Updates ersetzt werden kann (nur für Microsoft-Updates verfügbar).

- **Aufgaben zur Installation des Updates**

  Diese Registerkarte enthält eine Liste der Aufgaben, deren Bereiche die Installation des ausgewählten Updates enthalten. Mit dieser Registerkarte können Sie auch eine neue Aufgabe zur Remote-Installation für das Update erstellen.

So zeigen Sie die Statistik für eine Update-Installation an:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Programm-Update.
2. Klicken Sie auf **Statistik über die Statuszustände der Update-Installation**.

Das Diagramm mit dem Update-Installationsstatus wird angezeigt. Wenn Sie auf einen Status klicken, wird eine Liste der Geräte geöffnet, auf denen das Update den ausgewählten Status hat.

Sie können Informationen zu verfügbaren Software-Updates von Drittanbietern, einschließlich Microsoft, die auf dem ausgewählten verwalteten Windows-Gerät installiert ist, anzeigen.

Um eine Liste der verfügbaren Updates für Drittanbieter-Programme, die auf dem ausgewählten verwalteten Gerät installiert ist, anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, für das Sie die Updates für Drittanbieter-Programme anzeigen möchten.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

3. Klicken Sie im Eigenschaftenfenster des ausgewählten Geräts auf die Registerkarte **Erweitert**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Verfügbare Updates**. Wenn Sie nur installierte Updates anzeigen möchten, aktivieren Sie die Option **Installierte Updates anzeigen**.

Die Liste der verfügbaren Updates für Drittanbieter-Programme für das ausgewählte Gerät wird angezeigt.

Liste der verfügbaren Software-Updates in eine Datei exportieren

Sie können die angezeigte Liste der Updates für Drittanbieter-Programme, einschließlich der Software von Microsoft, in eine CSV- oder TXT-Datei exportieren. Diese Dateien können Sie beispielsweise an Ihren Informationssicherheitsmanager senden oder zu Statistikzwecken speichern.

Um die Liste der verfügbaren Updates für die Drittanbieter-Programme, die auf allen verwalteten Geräten installiert sind, in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Software-Updates**.

   Die Seite enthält eine Liste der verfügbaren Updates für die Drittanbieter-Programme, die auf allen verwalteten Geräten installiert sind.

2. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format für den Export bevorzugt wird.

Die Datei mit der Liste der verfügbaren Updates für Drittanbieter-Programme, einschließlich der Software von Microsoft, wird auf das momentan von Ihnen verwendete Gerät heruntergeladen.

Um die Liste der verfügbaren Updates für die Drittanbieter-Programme, die auf dem ausgewählten verwalteten Gerät installiert sind, in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Liste der auf dem verwalteten Gerät verfügbaren Updates für Drittanbieter-Programme.

2. Wählen Sie die Programm-Updates aus, die Sie exportieren möchten.

   Überspringen Sie diesen Schritt, wenn Sie eine vollständige Liste der Programm-Updates exportieren möchten.

   Wenn Sie eine vollständige Liste der Programm-Updates exportieren möchten, werden nur die auf der aktuellen Seite angezeigten Updates exportiert.

   Wenn Sie nur installierte Updates exportieren möchten, aktivieren Sie das Kontrollkästchen **Installierte Updates anzeigen**.

3. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format für den Export bevorzugt wird.

Die Datei mit der Liste der Updates für Drittanbieter-Programme, einschließlich der Software von Microsoft, die auf dem ausgewählten verwalteten Gerät installiert sind, wird auf das derzeit verwendete Gerät heruntergeladen.

Genehmigen und Ablehnen der Updates für Drittanbieter-Anwendungen

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* anpassen, können Sie eine Regel erstellen, die einen bestimmten Status für zu installierende Updates voraussetzt. Eine Update-Regel kann beispielsweise die Installation der folgenden Updates zulassen:

- Nur genehmigte Updates
- Nur genehmigte und nicht definierte Updates
- Alle Updates unabhängig vom Update-Status

Sie können Updates, die installiert werden müssen, genehmigen und Updates, die nicht installiert werden dürfen, ablehnen.

Bei einer geringen Menge an Updates ist das Verwenden des Status *Genehmigt* für die Verwaltung der Installation der Updates ist effizient. Für die Verwaltung vieler Updates können Sie die Regeln verwenden, die Sie in der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* konfigurieren können. Es wird empfohlen, den Status *Genehmigt* nur für die Updates zu setzen, die nicht den in den Regeln konfigurierten Kriterien entsprechen. Wenn Sie große Mengen an Updates manuell genehmigen, verringert sich die Leistungsfähigkeit des Administrationsservers, was zu einer Überlastung des Servers führen kann.

Um ein oder mehrere Updates zu genehmigen oder abzulehnen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Patch-Management → Software-Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

2. Wählen Sie die Updates aus, die Sie genehmigen oder ablehnen möchten.

3. Klicken Sie auf **Genehmigen**, um die ausgewählten Updates zu genehmigen, oder auf **Ablehnen**, um die ausgewählten Updates abzulehnen.

   Als Standard gilt der Wert *Nicht festgestellt*.

Die ausgewählten Updates haben die Status, die Sie definiert haben.

Optional können Sie den Genehmigungsstatus in den Eigenschaften eines bestimmten Updates ändern.

So genehmigen Sie ein Update in dessen Eigenschaften oder lehnen ein Update ab:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Patch-Management → Software-Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

2. Klicken Sie auf den Namen des Updates, das Sie genehmigen oder ablehnen möchten.

   Das Fenster mit den Update-Eigenschaften wird geöffnet.

3. Legen Sie im Abschnitt **Allgemein** durch das Ändern der Option **Status der Update-Genehmigung** einen Status für das Update fest. Sie können entweder den Status *Genehmigt*, *Abgelehnt* oder *Nicht definiert* festlegen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Das ausgewählte Update hat den Status, den Sie definiert haben.

Wenn Sie den Status **Deaktiviert** für Software-Updates von Drittanbietern angeben, werden die Updates nicht auf den Geräten installiert, auf denen sie vorgesehen waren, aber auf denen sie noch nicht installiert wurden. Auf den Geräten, auf denen die Updates bereits installiert wurden, bleiben diese auch weiterhin. Wenn Sie diese löschen müssen, können Sie dies manuell lokal vornehmen.

Erstellen der Aufgabe "Windows-Updates synchronisieren"

Die Aufgabe *Windows-Updates synchronisieren* ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Die Aufgabe *Windows-Updates synchronisieren* ist erforderlich, wenn Sie den Administrationsserver als WSUS-Server verwenden möchten. In diesem Fall lädt der Administrationsserver Windows-Updates in die Datenbank herunter und stellt die Updates für Windows Update auf Client-Geräten im zentralisierten Modus über Administrationsagenten bereit. Wenn im Netzwerk kein WSUS-Server verwendet wird, lädt jedes Client-Gerät die Microsoft-Updates selbständig von externen Servern herunter.

Die Aufgabe *Windows-Updates synchronisieren* lädt nur Metadaten von den Microsoft-Servern herunter. Kaspersky Security Center lädt nur die Updates, die Sie zur Installation auswählen, herunter, wenn Sie eine Update-Installationsaufgabe ausführen.

Während der Ausführung der Aufgabe **Windows-Updates synchronisieren**, erhält das Programm eine Liste der aktuellen Updates vom Update-Server von Microsoft. Danach erstellt Kaspersky Security Center eine Liste der veralteten Updates. Beim folgenden Start der Aufgabe **Suche nach Schwachstellen und erforderlichen Updates** kennzeichnet Kaspersky Security Center die veralteten Updates und bestimmt den Zeitpunkt der Entfernung. Beim folgenden Start der Aufgabe **Windows-Updates synchronisieren** werden die Updates gelöscht, die vor 30 Tagen zum Entfernen gekennzeichnet wurden. Kaspersky Security Center führt ferner eine zusätzliche Untersuchung für die Entfernung von veralteten Erneuerungen durch, die vor mehr als 180 Tagen gekennzeichnet wurden.

Nach Abschluss der Aufgabe **Windows-Updates synchronisieren** und Entfernung der veralteten Updates können die Hash-Codes der Dateien der entfernten Updates sowie die ihnen entsprechenden Dateien in der Datenbank im Ordner %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles bleiben, falls sie zuvor heruntergeladen wurden. Mithilfe der Aufgabe **Wartung des Administrationsservers** können Sie diese veralteten Einträge aus der Datenbank und den entsprechenden Dateien entfernen.

So erstellen Sie die Aufgabe Windows-Updates synchronisieren:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Windows-Updates synchronisieren**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Aktivieren Sie die Option **Express-Installationsdateien herunterladen**, wenn die Express-Update-Dateien beim Ausführen der Aufgabe heruntergeladen werden sollen.

   Wenn Kaspersky Security Center die Updates mit den Servern von Microsoft Windows Update Servers synchronisiert, werden Informationen über alle Dateien in der Datenbank des Administrationsservers gespeichert. Ferner werden alle Dateien, die für das Update notwendig sind, bei der Interaktion mit dem Windows Update-Agenten auf das Laufwerk heruntergeladen. Insbesondere speichert Kaspersky Security Center Informationen über die Updatedateien für die Expressinstallation in der Datenbank und lädt sie bei Bedarf. Wenn Sie Updatedateien für Expressinstallation herunterladen wird der freie Speicherplatz auf dem Laufwerk verringert.

   Um eine Verringerung des Speicherplatzes zu verhindern und den Datenverkehr zu reduzieren, deaktivieren Sie die Option **Express-Installationsdateien herunterladen**.

6. Wählen Sie das Programm aus, für das Sie Updates herunterladen möchten.

   Wenn das Kontrollkästchen **Alle Programme** aktiviert ist, werden die Updates für alle vorhandenen Programme, sowie für jene Programme heruntergeladen, die möglicherweise in Zukunft vorhanden sein könnten.

7. Wählen Sie die Kategorien von Updates aus, die Sie auf den Administrationsserver herunterladen möchten.

   Wenn das Kontrollkästchen **Alle Kategorien** aktiviert ist, werden die Updates für alle vorhandenen Update-Kategorien, sowie für jene Kategorien heruntergeladen, die möglicherweise in Zukunft vorhanden sein könnten.

8. Wählen Sie die Lokalisierungssprachen der Updates aus, die Sie auf den Administrationsserver herunterladen möchten. Wählen Sie eine der folgenden Varianten aus:

   - **Alle Sprachen (einschließlich neuer) herunterladen**

     Wurde diese Option ausgewählt, werden alle verfügbaren Sprachversionen der Updates auf den Administrationsserver heruntergeladen. Diese Variante ist standardmäßig ausgewählt.

   - **Ausgewählte Sprachen herunterladen**

     Wurde diese Option ausgewählt, können Sie in der Liste Sprachen zur Lokalisierung von Updates auswählen, die auf den Administrationsserver heruntergeladen werden sollen.

9. Geben Sie an, welches Konto beim Ausführen der Aufgabe verwendet werden soll. Wählen Sie eine der folgenden Varianten aus:

   - **Standardbenutzerkonto**

     Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

     Diese Variante ist standardmäßig ausgewählt.

   - **Benutzerkonto festlegen**

     Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

10. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

11. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

12. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

13. Geben Sie im Fenster mit den Aufgabeneigenschaften die passenden allgemeinen Aufgabeneinstellungen an.

14. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.

Automatisches Aktualisieren von Drittanbieter-Programmen

Einige Drittanbieter-Programme können automatisch aktualisiert werden. Der Hersteller des jeweiligen Programms legt fest, ob das Programm die Auto-Update-Funktion unterstützt oder nicht. Wenn das auf einem verwalteten Gerät installierte Drittanbieter-Programm Auto-Update unterstützt, können Sie die Auto-Update-Einstellungen in den Programmeinstellungen konfigurieren. Nach einer Änderung der Auto-Update-Option wenden die Administrationsagenten die neuen Einstellungen auf alle verwalteten Geräte an, auf denen das Programm installiert ist.

Die Auto-Update-Einstellung ist von den anderen Objekten und Einstellungen der Funktionen für Schwachstellen- und Patch-Management unabhängig. So hängt diese Einstellung beispielsweise nicht vom Genehmigungsstatus eines Updates oder von den Aufgaben zur Update-Installation, wie *Erforderliche Updates installieren und Schwachstellen schließen*, *Windows-Updates installieren* und *Schwachstellen schließen* ab.

Um die Auto-Update-Einstellung für ein Drittanbieter-Programm zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.
2. Klicken Sie auf den Namen des Programms, für das Sie die Auto-Update-Einstellung ändern wollen.

   Um die Suche zu erleichtern, können Sie Liste mittels der Spalte **Status des automatischen Updates** filtern.

   Das Fenster mit den Programmeinstellungen wird geöffnet.
3. Legen Sie im Abschnitt **Allgemein** einen Wert für die folgende Einstellung fest:

   Status des automatischen Updates

   Wählen Sie eine der folgenden Varianten aus:

   - **Nicht definiert**

     Die Auto-Update-Funktion ist deaktiviert. Kaspersky Security Center installiert Updates für Drittanbieter-Programme unter Verwendung der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen*, *Windows-Updates installieren*, und *Schwachstellen schließen*.

   - **Zugelassen**

     Nachdem der Hersteller ein Update für das Programm veröffentlicht hat, wird es automatisch auf den verwalteten Geräten installiert. Es sind keine weiteren Aktionen erforderlich.

   - **Blockiert**

     Die Programm-Updates werden nicht automatisch installiert. Kaspersky Security Center installiert Updates für Drittanbieter-Programme unter Verwendung der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen*, *Windows-Updates installieren*, und *Schwachstellen schließen*.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Die Auto-Update-Option wird auf das ausgewählte Programm angewendet.

Schließen von Schwachstellen in Programmen von Drittanbietern

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center beschrieben, die sich auf das Schließen von Schwachstellen in den Programmen beziehen, die auf verwalteten Geräten installierten sind.

Szenario: Finden und Schließen von Schwachstellen in Programmen von Drittanbietern

Dieser Abschnitt enthält ein Szenario zum Auffinden und Beheben von Schwachstellen auf verwalteten Geräten unter Windows. Sie können Schwachstellen im Betriebssystem und in Drittanbieter-Programmen, einschließlich der Software von Microsoft, finden und schließen.

Erforderliche Vorrausetzungen

- Kaspersky Security Center ist in Ihrer Organisation bereitgestellt.
- Sie haben in Ihrer Organisation verwaltete Geräte, auf denen Windows ausgeführt wird.
- Damit der Administrationsserver die folgenden Aufgaben ausführen kann, ist eine Internetverbindung erforderlich:
  - Erstellen einer Liste empfohlener Korrekturen für Schwachstellen in Software von Microsoft. Die Liste wird von Kaspersky-Spezialisten erstellt und regelmäßig aktualisiert.
  - Beheben von Schwachstellen in anderer Software von Drittanbietern als Microsoft-Software.

Schritte

Das Erkennen und Schließen von Schwachstellen in Programmen erfolgt schrittweise:

1. **Scannen nach Schwachstellen in den auf den verwalteten Geräten installierten Programmen**

   Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um Schwachstellen in den auf den verwalteten Geräten installierten Programmen zu suchen. Nach Abschluss dieser Aufgabe erhält Kaspersky Security Center eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Software von Drittanbietern, die auf den Geräten installiert ist, die Sie in den Eigenschaften der Aufgabe angegeben haben.

   Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch vom Schnellstartassistent des Kaspersky Security Centers erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, starten Sie ihn jetzt oder erstellen Sie die Aufgabe manuell.

   Anleitung:

   - Verwaltungskonsole: Schwachstellensuche in Programmen, Zeitplan erstellen für die Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"
   - Kaspersky Security Center Web Console: Aufgabe Suche nach Schwachstellen und erforderlichen Updates erstellen, Einstellungen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"

2. **Analysieren der Liste der erkannten Schwachstellen in Programmen**

   Zeigen Sie die Liste **Schwachstellen in Programmen** an und entscheiden Sie, welche Schwachstellen in Programmen behoben werden sollen. Um detaillierte Informationen über alle Schwachstellen anzuzeigen, klicken Sie in der Liste auf den Namen der Schwachstelle. Für jede Schwachstelle in der Liste können Sie auch eine Statistik über die Schwachstelle auf den verwalteten Geräten anzeigen.

Anleitung:

- Verwaltungskonsole: Anzeigen von Informationen zu Schwachstellen in Programmen, Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten
- Kaspersky Security Center Web Console: Informationen über Schwachstellen in Programmen anzeigen, Statistik über Schwachstellen auf verwalteten Geräten anzeigen

3 Konfigurieren von Korrekturen für Schwachstellen

Wenn Schwachstellen in Programmen erkannt werden, können Sie mithilfe der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* oder *Schwachstellen schließen* die Schwachstellen in Programmen auf den verwalteten Geräten schließen.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Drittanbieter-Programmen, einschließlich der Software von Microsoft, die auf den verwalteten Geräten installiert ist, zu aktualisieren und zu beheben. Mit dieser Aufgabe können Sie mehrere Updates installieren und mehrere Schwachstellen nach bestimmten Regeln beheben. Beachten Sie, dass diese Aufgabe nur erstellt werden kann, wenn Sie eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" haben. Um Schwachstellen in Programmen zu beheben, verwendet die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die empfohlenen Programm-Updates.

Die Aufgabe *Schwachstellen schließen* erfordert keine Lizenz-Option für die Funktion "Schwachstellen- und Patch-Management". Um die Aufgabe zu verwenden, müssen Sie manuell benutzerdefinierte Korrekturen angeben, um die Schwachstellen in Drittanbieter-Programmen zu beheben, die in den Aufgabeneinstellungen aufgeführt sind. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Microsoft-Programme und die benutzerdefinierten Korrekturen für Drittanbieter-Programme.

Sie können entweder den Assistenten für das Schließen von Schwachstellen starten, der automatisch eine dieser Aufgaben erstellt, oder Sie können eine dieser Aufgaben manuell erstellen.

Anleitung:

- Verwaltungskonsole: Auswählen von individuellen Korrekturen für Schwachstellen von Drittanbieter-Programmen, Schließen von Schwachstellen in Programmen
- Kaspersky Security Center Web Console: Auswählen von individuellen Korrekturen für Schwachstellen in Drittanbieter-Programmen, Schwachstellen in Drittanbieter-Programmen beheben, Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen

4 Planen der Aufgaben

Um sicherzustellen, dass die Liste der Schwachstellen immer auf dem neuesten Stand ist, planen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* so, dass sie regelmäßig automatisch ausgeführt wird. Die empfohlene durchschnittliche Häufigkeit ist einmal pro Woche.

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie festlegen, dass sie mit der gleichen Häufigkeit ausgeführt wird wie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* oder seltener. Beachten Sie beim planen der Aufgabe *Schwachstellen schließen*, dass Sie vor jedem Start der Aufgabe entweder Patches für Microsoft-Programme auswählen oder Patches für Drittanbieterprogramme angeben müssen.

Stellen Sie beim Planen der Aufgaben sicher, dass die Aufgabe zum Beheben von Schwachstellen erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen ist.

5 Ignorieren von Schwachstellen in Programmen (optional)

Sie können ggf. Schwachstellen in Programmen auf allen verwalteten Geräten oder nur auf den ausgewählten verwalteten Geräten ignorieren.

Anleitung:

- Verwaltungskonsole: Ignorieren von Schwachstellen in Programmen
- Kaspersky Security Center Web Console: Ignorieren von Schwachstellen in Programmen

6. **Aufgabe zum Schließen von Schwachstellen ausführen**

   Starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Schwachstelle schließen*. Stellen Sie nach Abschluss der Aufgabe sicher, dass sie in der Liste den Status *Erfolgreich abgeschlossen* hat.

7. **Bericht über die Ergebnisse des Schließens von Schwachstellen in Programmen erstellen (optional)**

   Generieren Sie den Bericht über Schwachstellen, um detaillierte Statistiken zu den behobenen Schwachstellen anzuzeigen. Der Bericht enthält Informationen über Schwachstellen in Programmen, die nicht behoben wurden. Dort können Sie sich darüber informieren, wie Sie in Ihrem Unternehmen nach Schwachstellen in Drittanbieter-Programmen, einschließlich der Software von Microsoft, suchen und solche Schwachstellen beheben können.

   Anleitung:

   - Verwaltungskonsole: Bericht erstellen und anzeigen
   - Kaspersky Security Center Web Console: Erzeugen und Anzeigen von Berichten

8. **Überprüfen der Konfiguration zum Finden und Schließen von Schwachstellen in Drittanbieter-Programmen**

   Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

   - Abrufen und Überprüfen der Liste von Schwachstellen in Programmen auf verwalteten Geräten
   - Ignorieren von Schwachstellen in Programmen, falls gewünscht
   - Konfigurieren der Aufgabe zum Schließen von Schwachstellen
   - Planen der Aufgaben zum Finden und Schließen von Schwachstellen in Programmen, sodass dass sie nacheinander gestartet werden
   - Überprüfen, ob die Aufgabe zum Schließen von Schwachstellen in Programmen ausgeführt wurde

Ergebnisse

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt und angepasst haben, werden die Schwachstellen auf den verwalteten Geräten automatisch behoben. Beim Ausführen der Aufgabe wird die Liste der verfügbaren Programm-Updates mit den Regeln abgeglichen, die in den Aufgabeneinstellungen angegeben sind. Alle Programm-Updates, welche die Kriterien der Regeln erfüllen, werden in die Datenverwaltung des Administrationsservers heruntergeladen und werden installiert, um die Schwachstellen in Programmen zu beheben.

Wenn Sie die Aufgabe *Schwachstellen schließen* erstellt haben, werden nur Schwachstellen in der Software von Microsoft geschlossen.

Über das Suchen und Schließen von Schwachstellen in Programmen

Kaspersky Security Center erkennt und behebt Schwachstellen in Programmen auf verwalteten Geräten, auf denen Microsoft Windows-Betriebssysteme ausgeführt werden. Schwachstellen werden im Betriebssystem und in Software von Drittanbietern, einschließlich Microsoft-Software, erkannt.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Software-Schwachstellen suchen

Kaspersky Security Center verwendet Merkmale aus der Datenbank mit bekannten Schwachstellen, um Schwachstellen in Programmen zu finden. Diese Datenbank wird von Kaspersky-Spezialisten erstellt. Sie enthält Informationen zu Schwachstellen, z. B. eine Beschreibung, das Datum der Erkennung und die Signifikanz der Schwachstelle. Informationen über Schwachstellen in Programmen finden Sie auf der Website von Kaspersky.

Kaspersky Security Center verwendet die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Schwachstellen in Programmen zu finden.

In bestimmten Fällen können Schwachstellen, die in einem Microsoft Windows-Betriebssystem gefunden wurden, mit einer der folgenden Methoden geschlossen werden:

- Installieren eines Updates für das Betriebssystem.
- Upgrade des Betriebssystems auf eine aktuellere Version (z. B. von Windows 10 auf Windows 11).

In diesem Szenario zeigt Kaspersky Security Center zwei Einträge für dieselbe Schwachstelle an.

Beheben von Schwachstellen in Programmen

Zum Beheben von Schwachstellen in Programmen verwendet Kaspersky Security Center die Programm-Updates der Programmhersteller. Die Metadaten des Programm-Updates werden als Ergebnis der Ausführung der folgenden Aufgabe in die Datenverwaltung des Administrationsservers heruntergeladen:

- *Download von Updates in die Datenverwaltung des Administrationsservers*. Diese Aufgabe dient dazu, Metadaten der Updates für die Software von Kaspersky und für Drittanbieter-Programme herunterzuladen. Diese Aufgabe wird automatisch vom Schnellstartassistent des Kaspersky Security Centers erstellt. Sie können die Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers manuell erstellen.
- *Windows-Updates synchronisieren*. Diese Aufgabe dient dazu, Metadaten der Updates für die Software von Microsoft herunterzuladen.

Software-Updates zur Behebung von Schwachstellen können in Form von vollständigen Programmpaketen oder Patches bereitgestellt werden. Programm-Updates, die Schwachstellen in Programmen beheben, werden als *Korrekturen* bezeichnet. *Empfohlene Korrekturen* sind solche, deren Installation von Kaspersky-Spezialisten empfohlen wird. *Individuelle Korrekturen* sind solche, die manuell für die Installation durch Benutzer ausgewählt werden. Um eine Benutzerkorrektur zu installieren, müssen Sie ein Installationspaket erstellen, das diese Korrektur enthält.

Wenn Sie über die Lizenz für Kaspersky Security Center mit der Schwachstellen- und Patch-Management-Funktion verfügen, um Schwachstellen in Programmen zu schließen, können Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* verwenden. Diese Aufgabe behebt automatisch mehrere Schwachstellen, indem empfohlene Korrekturen installiert werden. Für diese Aufgabe können Sie bestimmte Regeln manuell konfigurieren, um mehrere Schwachstellen zu beheben.

Wenn Sie nicht über die Lizenz für Kaspersky Security Center mit der Schwachstellen- und Patch-Management-Funktion verfügen, um Schwachstellen in Programmen zu schließen, können Sie die Aufgabe *Schwachstellen schließen* verwenden. Mithilfe dieser Aufgabe können Sie Schwachstellen beheben, indem empfohlene Korrekturen für die Software von Microsoft und Benutzerkorrekturen für andere Drittanbieter-Programme installiert werden.

Aus Sicherheitsgründen werden alle Programm-Updates von Drittanbietern, die Sie mittels der Funktion "Schwachstellen- und Patch-Management" installieren, automatisch von den Kaspersky-Technologien auf Schadsoftware untersucht. Die Technologien werden zur automatischen Untersuchung von Dateien verwendet und umfassen die Virensuche, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung sowie Machine-Learning-Methoden.

Kaspersky-Experten führen keine manuelle Analyse von Updates für Drittanbieter-Programme durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten in derartigen Updates weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen, noch führen sie an ihnen zusätzliche Analysen durch, die über die oben genannten hinausgehen.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie eine Drittanbieter-Anwendung aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einer Drittanbieter-Anwendung beheben. Beispielsweise kann der Benutzer aufgefordert werden, die Drittanbieter-Anwendung zu schließen, wenn es gerade geöffnet ist.

Zum Schließen bestimmter Software-Schwachstellen müssen Sie bei Aufforderung den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren. Wenn Sie die EULA ablehnen, kann die Schwachstelle nicht geschlossen werden.

Schwachstellen in Drittanbieter-Programmen schließen

Nachdem Sie die Liste mit den Schwachstellen in Programmen abgerufen haben, können Sie die Schwachstellen in Programmen auf den verwalteten Windows-Geräten beheben. Das Schließen von Schwachstellen im Betriebssystem und in Drittanbieter-Programmen, einschließlich in der Software von Microsoft, ist mithilfe der Aufgabe *Schwachstellen schließen* oder der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* möglich.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, ein momentan geöffnetes Drittanbieter-Programm zu schließen.

Optional können Sie eine Aufgabe erstellen, um Schwachstellen in Programmen auf folgende Weise zu schließen:

- Öffnen Sie die Schwachstellenliste und geben Sie an, welche Schwachstellen geschlossen werden sollen.

  Dadurch wird eine neue Aufgabe zum Schließen von Software-Schwachstellen erstellt. Sie können die ausgewählten Schwachstellen auch zu einer vorhandenen Aufgabe hinzufügen.

- Führen Sie den Assistenten für das Schließen von Schwachstellen aus.

Der Assistent zum Schließen von Schwachstellen ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Der Assistent vereinfacht die Erstellung und Konfiguration einer Aufgabe zum Schließen von Schwachstellen und ermöglicht es Ihnen, die Erstellung redundanter Aufgaben zu vermeiden, die dieselben zu installierenden Updates enthalten.

Schließen von Schwachstellen in Programmen mithilfe der Schwachstellenliste

Um Schwachstellen in Programmen zu beheben, gehen Sie wie folgt vor:

1. Öffnen Sie eine der Listen mit Schwachstellen:

   - Um die allgemeine Schwachstellenliste zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.
   - Um die Schwachstellenliste für ein verwaltetes Gerät zu öffnen, wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte** → <Gerätename> → **Erweitert** → **Schwachstellen in Programmen**.
   - Um die Schwachstellenliste für ein bestimmtes Programm zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry** → <Programmname> → **Schwachstellen**.

   Eine Seite mit der Liste von Schwachstellen in Drittanbieter-Programmen wird angezeigt.

2. Wählen Sie in der Liste eine oder mehrere Schwachstellen aus und klicken Sie anschließend auf **Schwachstelle schließen**.

   Wenn das empfohlene Update zum Schließen der Schwachstelle nicht vorhanden ist, wird dies gemeldet.

   Zum Schließen bestimmter Software-Schwachstellen müssen Sie bei Aufforderung den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren. Wenn Sie die EULA ablehnen, kann die Schwachstelle nicht geschlossen werden.

3. Wählen Sie eine der folgenden Varianten aus:

   - **Neue Aufgabe**

     Der Assistent für das Erstellen einer Aufgabe wird gestartet. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management verfügen, wird die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* vorausgewählt. Wenn Sie nicht über die Lizenz verfügen, wird die Aufgabe *Schwachstellen schließen* vorausgewählt. Folgen Sie den Schritten des Assistenten, um die Erstellung der Aufgabe abzuschließen.

   - **Schwachstelle schließen (Regel zur angegebenen Aufgabe hinzufügen)**

     Wählen Sie eine Aufgabe, der Sie die ausgewählten Schwachstellen hinzufügen wollen. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management Lizenz für Schwachstellen- und Patch-Management verfügen, wählen Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* aus. Eine neue Regel zum Schließen der ausgewählten Schwachstellen wird der ausgewählten Aufgabe automatisch hinzugefügt. Wenn Sie nicht über die Lizenz verfügen, wählen Sie die Aufgabe *Schwachstellen schließen* aus. Die ausgewählten Schwachstellen werden den Aufgabeneigenschaften hinzugefügt.

Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wenn Sie sich entschieden haben, eine Aufgabe zu erstellen, so wird diese Aufgabe in der Aufgabenliste unter **Assets (Geräte)** → **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Schwachstellen zu einer vorhandenen Aufgabe hinzuzufügen, werden die Schwachstellen in den Aufgabeneigenschaften gespeichert.

Um Schwachstellen in Drittanbieter-Programmen zu schließen, starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Schwachstellen schließen*. Wenn Sie die Aufgabe *Schwachstellen schließen* erstellt haben, müssen Sie die Programm-Updates manuell angeben, um die in den Aufgabeneinstellungen aufgelisteten Schwachstellen in Programmen zu schließen.

Schließen von Schwachstellen in Programmen mithilfe des Assistenten zum Schließen von Schwachstellen

Der Assistent für das Schließen von Schwachstellen ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

So schließen Sie Software-Schwachstellen mithilfe des Assistenten für das Schließen von Schwachstellen:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Eine Seite mit der Liste von Schwachstellen in Drittanbieter-Programmen, die auf den verwalteten Geräten installiert sind, wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben der Schwachstelle, die Sie schließen möchten.

3. Klicken Sie auf die Schaltfläche **Assistent zum Schließen von Schwachstellen starten**.

   Der Assistent für das Schließen von Schwachstellen wird geöffnet. Die Seite **Aufgabe zum Schließen von Schwachstellen auswählen** zeigt Ihnen die Liste aller existierenden Aufgaben der folgenden Arten an:

   - *Erforderliche Updates installieren und Schwachstellen schließen*
   - *Windows-Updates installieren*
   - *Schwachstellen schließen*

   Die beiden letzteren Aufgabenarten können Sie nicht modifizieren, um neue Updates zu installieren. Um neue Updates zu installieren, können Sie nur die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* verwenden.

4. Wenn der Assistent nur die Aufgaben anzeigen soll, mit denen die von Ihnen ausgewählte Schwachstelle geschlossen werden soll, aktivieren Sie die Option **Nur Aufgaben anzeigen, die diese Schwachstelle schließen**.

5. Wählen Sie, was Sie tun möchten:

- Um eine Aufgabe zu starten, aktivieren Sie das Kontrollkästchen neben dem Aufgabennamen und klicken auf die Schaltfläche **Starten**.

- So fügen Sie einer vorhandenen Aufgabe eine neue Regel hinzu:

  a. Aktivieren Sie das Kontrollkästchen neben dem Aufgabennamen und klicken Sie auf die Schaltfläche **Regel hinzufügen**.

  b. Konfigurieren Sie auf der sich öffnenden Seite die neue Regel:

  - **Regel zum Schließen aller Schwachstellen der ausgewählten Signifikanz**

    Manchmal können sich Programm-Updates negativ auf die Benutzererfahrung eines Programms auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

    Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

    Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

    Diese Option ist standardmäßig deaktiviert.

  - **Regel zum Schließen von Schwachstellen mithilfe von Updates des gleichen Typs wie das für die ausgewählte Schwachstelle empfohlene Update** (nur für Schwachstellen in Software von Microsoft verfügbar)

  - **Regel zum Schließen von Schwachstellen in Programmen des ausgewählten Anbieters** (nur für Schwachstellen in Drittanbieter-Programmen verfügbar)

  - **Regel zum Schließen von Schwachstellen in allen Versionen des ausgewählten Programms** (nur für Schwachstellen in Drittanbieter-Programmen verfügbar)

  - **Regel zum Schließen der ausgewählten Schwachstelle**

  - **Updates zum Schließen der ausgewählten Schwachstelle freigeben**

    Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

    Diese Option ist standardmäßig deaktiviert.

  c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

- So erstellen Sie eine Aufgabe:

  a. Klicken Sie auf **Neue Aufgabe**.

  b. Konfigurieren Sie auf der sich öffnenden Seite die neue Regel:

  - **Regel zum Schließen aller Schwachstellen der ausgewählten Signifikanz**

Manchmal können sich Programm-Updates negativ auf die Benutzererfahrung eines Programms auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

Diese Option ist standardmäßig deaktiviert.

- **Regel zum Schließen von Schwachstellen mithilfe von Updates des gleichen Typs wie das für die ausgewählte Schwachstelle empfohlene Update** (nur für Schwachstellen in Software von Microsoft verfügbar)
- **Regel zum Schließen von Schwachstellen in Programmen des ausgewählten Anbieters** (nur für Schwachstellen in Drittanbieter-Programmen verfügbar)
- **Regel zum Schließen von Schwachstellen in allen Versionen des ausgewählten Programms** (nur für Schwachstellen in Drittanbieter-Programmen verfügbar)
- **Regel zum Schließen der ausgewählten Schwachstelle**
- **Updates zum Schließen der ausgewählten Schwachstelle freigeben**

  Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Wenn Sie sich entschieden haben, eine Aufgabe zu starten, können Sie den Assistenten schließen. Die Aufgabe wird im Hintergrundmodus durchgeführt. Es sind keine weiteren Aktionen erforderlich.

Wenn Sie sich entschieden haben, die Regel zu einer vorhandenen Aufgabe hinzuzufügen, wird das Fenster mit den Aufgabeneigenschaften geöffnet. Die neue Regel wurde den Aufgabeneigenschaften bereits hinzugefügt. Sie können die Regel oder andere Aufgabeneigenschaften anzeigen und anpassen. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wenn Sie eine Aufgabe erstellen möchten, fahren Sie im Assistenten für das Erstellen einer Aufgabe mit der Erstellung der Aufgabe fort. Die neue Regel, die Sie im Assistenten für das Schließen von Schwachstellen hinzugefügt haben, wird im Assistenten für das Erstellen einer Aufgabe angezeigt. Wenn Sie den Assistenten abgeschlossen haben, wird die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* zur Aufgabenliste hinzugefügt.

Erstellen der Aufgabe "Schwachstellen schließen"

Die Aufgabe *Schwachstellen schließen* ermöglicht das Schließen von Schwachstellen in Programmen die auf verwalteten Windows-Geräten ausgeführt werden. Sie können Schwachstellen in Programmen in den Programmen von Drittanbietern, einschließlich Microsoft, schließen.

Wenn Sie nicht über die Lizenz für Schwachstellen- und Patch-Management verfügen, können Sie keine neuen Aufgaben des Typs *Schwachstellen schließen* erstellen. Um neue Schwachstellen zu schließen, können Sie diese zu einer bestehenden *Schwachstellen schließen*-Aufgabe hinzufügen. Wir empfehlen die Verwendung der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* statt der Aufgabe *Schwachstellen schließen*. Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ermöglicht es Ihnen, mehrere Updates zu installieren und mehrere Schwachstellen automatisch gemäß den von Ihnen definierten Regeln zu schließen.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, das Drittanbieter-Programm zu schließen, wenn es gerade geöffnet ist.

So erstellen Sie die Aufgabe Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Schwachstellen schließen**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen.

   Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.
6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Die Liste der Schwachstellen wird geöffnet.
7. Wählen Sie die Schwachstellen aus, die Sie schließen möchten, und klicken Sie auf **OK**.

   Schwachstellen in Programmen von Microsoft haben normalerweise empfohlene Korrekturen. Für sie sind keine zusätzlichen Aktionen erforderlich. Bei Schwachstellen in Software anderer Anbieter müssen Sie zunächst einen Benutzer-Fix für jede Schwachstelle angeben, die Sie schließen möchten. Danach können Sie diese Schwachstellen der Aufgabe *Schwachstellen schließen* hinzufügen.
8. Geben Sie Neustart-Einstellungen des Betriebssystems an:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

   - **Gerät neu starten**

     Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

- **Aufforderung regelmäßig wiederholen nach (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

9. Legen Sie die Benutzerkonto-Einstellungen fest:

- **Standardbenutzerkonto**

  Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

  Diese Variante ist standardmäßig ausgewählt.

- **Benutzerkonto festlegen**

  Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

- **Benutzerkonto**

  Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

- **Kennwort**

  Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

10. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

11. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

12. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

13. Geben Sie im Fenster mit den Aufgabeneigenschaften die passenden allgemeinen Aufgabeneinstellungen an.

14. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.

Erstellen der Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen"

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Drittanbieter-Programmen, einschließlich Microsoft, die auf den verwalteten Geräten installiert ist, zu aktualisieren und zu beheben. Mit dieser Aufgabe können Sie mehrere Updates installieren und mehrere Schwachstellen nach bestimmten Regeln beheben.

Sie haben eine der folgenden Möglichkeiten, um mithilfe der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* Updates zu installieren oder Schwachstellen zu schließen:

- Führen Sie den Assistenten für die Installation von Updates oder den Assistenten für das Schließen von Schwachstellen aus.
- Erstellen einer Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Fügen Sie eine Regel für die Update-Installation zu einer bestehenden Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* hinzu.

So erstellen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Erforderliche Updates installieren und Schwachstellen schließen**.

   Wenn die Aufgabe nicht angezeigt wird, prüfen Sie, ob Ihr Benutzerkonto über die Berechtigungen **Lesen**, **Ändern** und **Ausführen** für den Funktionsbereich **Systemverwaltung**: **Schwachstellen- und Patch-Management** verfügt. Sie könne die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen"* ohne diese Zugriffsrechte nicht erstellen und konfigurieren.

4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.

6. Geben Sie die Regeln für die Update-Installation und dann die folgenden Einstellungen an:

   - **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen**

     Ist diese Option aktiviert, so werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Andernfalls werden Updates nach einem Zeitplan installiert.

     Verwenden Sie diese Option, wenn die Installation von Updates die Geräteleistung beeinträchtigen könnte.

     Diese Option ist standardmäßig deaktiviert.

   - **Erforderliche allgemeine Systemkomponenten installieren**

     Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

     Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

     Diese Option ist standardmäßig deaktiviert.

   - **Installation einer neuen Programmversion beim Update zulassen**

     Ist diese Option aktiviert, so werden Updates erlaubt, wenn sie zur Installation einer neuen Version einer Softwareanwendung führen.

     Wenn diese Option deaktiviert ist, wird die Software nicht aktualisiert. Sie können dann neue Versionen der Software manuell oder über eine andere Aufgabe installieren. Sie können diese Option beispielsweise verwenden, wenn die Infrastruktur Ihres Unternehmens nicht von einer neuen Softwareversion unterstützt wird oder wenn Sie ein Update in einer Testinfrastruktur überprüfen möchten.

     Diese Option ist standardmäßig aktiviert.

     > Aktualisieren einer Anwendung kann zu Fehlern bei abhängigen Anwendungen führen, die auf Client-Geräten installiert sind.

   - **Updates auf das Gerät herunterladen, ohne sie zu installieren**

     Wenn diese Option aktiviert ist, lädt die Anwendung Updates auf das Gerät herunter, installiert sie jedoch nicht automatisch. Sie können die heruntergeladenen Updates dann manuell installieren.

     Microsoft-Updates werden in den Windows-Systemspeicher heruntergeladen. Updates für Drittanbieter-Anwendungen (Anwendungen, die von den Software-Herstellern Kaspersky oder Microsoft stammen) werden in den Ordner heruntergeladen, der im Feld **Updates herunterladen nach** angegeben ist.

     Wenn diese Option deaktiviert ist, werden die Updates automatisch auf dem Gerät installiert.

     Diese Option ist standardmäßig deaktiviert.

- **Updates herunterladen nach**

  Dieser Ordner wird verwendet, um Updates für Drittanbieter-Anwendungen (Anwendungen, die nicht von den Software-Herstellern Kaspersky oder Microsoft stammen) herunterzuladen.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Dateien zur Ablaufverfolgung auch dann an, wenn das Erstellen von Dateien zur Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool Remote-Diagnose für Kaspersky Security Center durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

7. Geben Sie Neustart-Einstellungen des Betriebssystems an:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

- **Aufforderung regelmäßig wiederholen nach (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Wartezeit vor dem erzwungenen Schließen von Programmen in gesperrten Sitzungen (Min.)**

  Programme werden zwangsweise geschlossen, wenn das Benutzergerät gesperrt wird (automatisch nach einer bestimmten Inaktivitätsdauer oder manuell).

  Wenn diese Option aktiviert ist, werden Programme auf einem gesperrten Gerät nach Ablauf der im Eingabefeld angegebenen Zeitspanne automatisch geschlossen.

  Wenn diese Option deaktiviert ist, werden Programme auf einem gesperrten Gerät nicht geschlossen.

  Diese Option ist standardmäßig deaktiviert.

8. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

10. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

11. Geben Sie im Fenster mit den Aufgabeneigenschaften die passenden allgemeinen Aufgabeneinstellungen an.

12. Klicken Sie auf die Schaltfläche **Speichern**.

    Die Aufgabe wird erstellt und konfiguriert.

Wenn die Aufgabenergebnisse eine Warnung des Fehlers 0x80240033 "Windows Update Agent error 80240033 ("Lizenzbedingungen konnten nicht heruntergeladen werden.")" enthalten, können Sie dieses Problem über die Windows-Registrierung beheben.

Hinzufügen einer Regel für die Installation von Updates

Diese Funktion ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Beim Installieren von Programm-Updates oder beim Schließen von Schwachstellen in Programmen mittels der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* müssen Sie Regeln für die Update-Installation angeben. Diese Regeln bestimmen, welche Updates installiert und welche Schwachstellen geschlossen werden.

Die genauen Einstellungen hängen davon ab, ob Sie eine Regel für alle Updates, für Windows Update-Updates oder für Updates von Drittanbieter-Programmen (Programme von anderen Softwareherstellern als Kaspersky und Microsoft) hinzufügen. Beim Hinzufügen einer Regel für Windows Update-Updates oder Updates von Drittanbieter-Programmen können Sie bestimme Programme und Programmversionen auswählen, für die Sie Updates installieren möchten. Beim Hinzufügen einer Regel für alle Updates können Sie bestimmte Updates, die Sie installieren möchten, und Schwachstellen, die Sie mittels Installation von Updates schließen möchten, auswählen.

Sie können eine Regel für die Update-Installation auf folgende Arten hinzufügen:

- Durch Hinzufügen einer Regel beim Erstellen einer neuen Aufgabe des Typs Erforderliche Updates installieren und Schwachstellen schließen.
- Durch Hinzufügen einer Regel auf der Registerkarte **Programmeinstellungen** im Eigenschaftenfenster einer vorhandenen Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Durch Ausführen des Assistenten für die Installation von Updates oder des Assistenten für das Schließen von Schwachstellen.

Um eine neue Regel für alle Updates hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

2. Wählen Sie auf der Seite **Regeltyp** den Typ **Regel für alle Updates** aus.

3. Verwenden Sie auf der Seite **Allgemeine Kriterien** die Dropdown-Listen, um die folgenden Einstellungen festzulegen:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.
     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.
     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Updates** die Updates aus, die installiert werden sollen:

   - **Alle relevanten Updates installieren**

     Installieren Sie alle Programm-Updates, von denen die im Assistenten auf der Seite **Allgemeine Kriterien** aufgeführten Kriterien erfüllt werden. Standardmäßig ausgewählt.

   - **Nur Updates aus der Liste installieren**

     Es werden nur Programm-Updates installiert, die Sie in der Liste manuell auswählen. Diese Liste enthält alle verfügbaren Programm-Updates.

     Sie können beispielsweise in den folgenden Fällen bestimmte Updates auswählen: um deren Installation in einer Testumgebung zu überprüfen, um nur kritische Programme zu aktualisieren oder um nur bestimmte Programme zu aktualisieren.

     - **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

       Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

       Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

       Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

       Diese Option ist standardmäßig aktiviert.

5. Wählen Sie auf der Seite **Schwachstellen** jene Schwachstellen aus, die durch die Installation der ausgewählten Updates geschlossen werden:

   - **Alle Schwachstellen schließen, die den übrigen Kriterien entsprechen**

     Beheben Sie alle Schwachstellen, welche die Kriterien auf der Seite **Allgemeine Kriterien** des Assistenten erfüllen. Standardmäßig ausgewählt.

   - **Nur Schwachstellen aus der Liste schließen**

     Es werden nur Schwachstellen geschlossen, die Sie manuell aus der Liste auswählen. Diese Liste enthält alle gefundenen Schwachstellen.

     Sie können beispielsweise in den folgenden Fällen bestimmte Schwachstellen auswählen: um deren Schließen in einer Testumgebung zu überprüfen, um Schwachstellen nur in kritischen Apps zu schließen oder um Schwachstellen nur in bestimmten Programmen zu aktualisieren.

6. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie hinzufügen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem dem Abschließen des Assistenten für das Erstellen einer Regel wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgabe oder in den Aufgabeneigenschaften angezeigt.

Um eine neue Regel für Windows Update-Updates hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

2. Wählen Sie auf der Seite **Regeltyp** den Typ **Regel für Windows-Updates** aus.

3. Passen Sie auf der Seite **Allgemeine Kriterien** die folgenden Einstellungen an:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.
     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.
     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

   - **Schwachstellen schließen, deren MSRC-Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Anwendungen** die Programme und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Wählen Sie auf der Seite **Update-Kategorien** die Kategorien der Updates aus, die installiert werden sollen. Diese Kategorien entsprechen den Kategorien im Microsoft-Update-Katalog. Standardmäßig sind alle Kategorien ausgewählt.

6. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie hinzufügen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem dem Abschließen des Assistenten für das Erstellen einer Regel wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgabe oder in den Aufgabeneigenschaften angezeigt.

Um eine neue Regel für Updates von Drittanbieter-Programmen hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

2. Wählen Sie auf der Seite **Regeltyp** den Typ **Regel für Updates von Drittherstellern** aus.

3. Passen Sie auf der Seite **Allgemeine Kriterien** die folgenden Einstellungen an:

   - **Satz der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.

     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht festgestellt* installiert.

     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Anwendungen** die Programme und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie hinzufügen. Sie können diesen Namen später im Abschnitt Einstellungen des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem dem Abschließen des Assistenten für das Erstellen einer Regel wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgabe oder in den Aufgabeneigenschaften angezeigt.

Auswählen von Benutzerkorrekturen für Schwachstellen in Programmen von Drittanbietern

Zur Verwendung der Aufgabe *Schwachstellen schließen* müssen Sie die Programm-Updates manuell angeben, mit denen die in den Aufgabeneinstellungen angegeben Schwachstellen in den Drittanbieter-Programmen behoben werden sollen. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Software von Microsoft und individuelle Korrekturen für andere Drittanbieter-Programme. *individuelle Korrekturen* sind Programm-Updates zum Beheben von Schwachstellen, die vom Administrator manuell für die Installation ausgewählt werden.

So wählen Sie Benutzerkorrekturen für Schwachstellen in Software von Drittanbietern aus:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Auf der Seite wird die Liste der auf Client-Geräten erkannten Schwachstellen in Programmen angezeigt.

2. Klicken Sie in der Liste der Schwachstellen in Programmen auf den Link mit dem Namen der Software-Schwachstelle, für die Sie eine individuelle Korrektur angeben möchten.

   Das Eigenschaftenfenster der Schwachstelle wird geöffnet.

3. Wählen Sie im linken Fensterbereich den Abschnitt **Benutzerdefinierte und andere Patches**.

   Die Liste der Benutzerkorrekturen für die ausgewählte Software-Schwachstelle wird angezeigt.

4. Klicken Sie auf **Hinzufügen**.

   Eine Liste der verfügbaren Installationspakete wird angezeigt. Die Liste der angezeigten Installationspakete entspricht der Liste **Vorgänge** → **Datenverwaltung** → **Installationspakete**. Wenn Sie kein Installationspaket erstellt haben, das eine benutzerdefinierte Korrektur für die ausgewählte Schwachstelle enthält, können Sie das Paket jetzt mithilfe des "Assistenten für das Erstellen eines Installationspakets" erstellen.

5. Wählen Sie ein Installationspaket (bzw. Pakete) aus, in dem eine benutzerdefinierte Korrektur (bzw. benutzerdefinierte Korrekturen) für die Schwachstelle in dem Drittanbieter-Programm enthalten ist.

6. Klicken Sie auf **Speichern**.

Die Installationspakete, die Benutzerkorrekturen für die Software-Schwachstelle enthalten, werden angegeben. Bei Ausführung der Aufgabe *Schwachstellen schließen*, wird das Installationspaket installiert und die Software-Schwachstelle wird behoben.

Anzeigen von Informationen zu Schwachstellen in Programmen, die auf allen verwalteten Geräten erkannt wurden

Nachdem Sie die Software auf verwalteten Geräten auf Schwachstellen untersucht haben, können Sie die Liste der auf allen verwalteten Geräten erkannten Schwachstellen in Programmen anzeigen. Wenn Sie die Aufgabe für die Hierarchie der Administrationsserver ausführen, können Sie die Liste der verwalteten Geräte mit erkannten Schwachstellen nur für den ausgewählten Administrationsserver anzeigen.

Um eine Liste mit Schwachstellen in Programmen, die auf den verwalteten Geräten erkannt wurden, anzuzeigen, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

Auf der Seite wird die Liste der auf Client-Geräten erkannten Schwachstellen in Programmen angezeigt.

Sie können auch Bericht über Schwachstellen erstellen und anzeigen.

Sie können einen Filter angeben, um die Liste der Schwachstellen in Programmen anzuzeigen. Klicken Sie auf das Symbol **Filter**-Symbol (⚙) oben rechts in der Liste mit Schwachstellen in Programmen, um den Filter zu verwalten. Sie können auch einen der voreingestellten Filter aus der Dropdown-Liste **Vordefinierte Filter** oberhalb der Liste mit Schwachstellen in Programmen auswählen.

Sie können ausführliche Informationen über Schwachstellen über die Liste abrufen.

Um Informationen über eine Schwachstelle in einem Programm abzurufen, gehen Sie wie folgt vor:

Klicken Sie in der Liste mit Schwachstellen in Programmen auf den Link mit dem Namen der Schwachstelle.

Das Eigenschaftenfenster der Software-Schwachstelle wird geöffnet.

Anzeigen von Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden

Sie können Informationen zu Software-Schwachstellen, die auf dem ausgewählten verwalteten Windows-Gerät erkannt wurden, anzeigen.

So zeigen Sie die Liste der Software-Schwachstellen an, die auf dem ausgewählten verwalteten Gerät gefunden wurden:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, für das Sie erkannte Software-Schwachstellen anzeigen möchten.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

3. Klicken Sie im Eigenschaftenfenster des ausgewählten Geräts auf die Registerkarte **Erweitert**.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Schwachstellen in Programmen** aus.

   Die Liste der Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden, wird angezeigt.

So zeigen Sie die Eigenschaften der ausgewählten Schwachstelle an:

Klicken Sie in der Liste der Software-Schwachstellen auf den Link mit dem Namen der Schwachstelle.

Das Eigenschaftenfenster der ausgewählten Schwachstelle wird geöffnet.

Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten

Sie können eine Statistik für jede Software-Schwachstelle auf verwalteten Geräten anzeigen. Die Statistik wird als Diagramm angezeigt. Das Diagramm enthält die Anzahl der Geräte mit den folgenden Statusvarianten:

- *Ignoriert auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie in den Eigenschaften der Schwachstelle manuell die Option zum Ignorieren der Schwachstelle festgelegt haben.
- *Geschlossen auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn die Aufgabe zum Schließen der Schwachstelle erfolgreich abgeschlossen wurde.
- *Korrektur geplant auf <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie die Aufgabe zum Schließen der Schwachstelle erstellt haben, die Aufgabe jedoch noch nicht ausgeführt wurde.
- *Patch angewendet auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie ein Programm-Update zur Behebung der Schwachstelle manuell ausgewählt haben, die Schwachstelle jedoch dadurch nicht geschlossen wurde.
- *Korrektur erforderlich auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn die Schwachstelle nur auf einigen der verwalteten Geräten geschlossen wurde und auf den anderen verwalteten Geräten noch geschlossen werden muss.

So zeigen Sie die Statistik über Schwachstelle auf einem verwalteten Gerät an:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Patch-Management → Schwachstellen in Programmen**.

   Die Seite mit der Liste von Schwachstellen in Programmen auf den verwalteten Geräten wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben der zu schließenden Schwachstelle.
3. Klicken Sie auf die Schaltfläche **Statistik zu Schwachstellen auf Geräten**.

Ein Diagramm der Schwachstellenstatus wird angezeigt. Wenn Sie auf einen Status klicken, wird eine Liste der Geräte geöffnet, auf denen die Schwachstelle den ausgewählten Status hat.

Exportieren der Liste von Schwachstellen in Programmen in eine Datei

Sie können die angezeigte Liste der Schwachstellen in eine CSV- oder TXT-Datei exportieren. Diese Dateien können Sie beispielsweise an Ihren Informationssicherheitsmanager senden oder zu Statistikzwecken speichern.

Um eine Liste der Schwachstellen in Programmen, die auf allen verwalteten Geräten erkannt wurden, in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Patch-Management → Schwachstellen in Programmen**.

   Die Seite mit der Liste von Schwachstellen in Programmen auf den verwalteten Geräten wird angezeigt.

2. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format für den Export bevorzugt wird.

Die Datei mit der Liste der Schwachstellen in Programmen wird auf das Gerät heruntergeladen, das Sie gerade verwenden.

Um eine Liste der Schwachstellen in Programmen, die auf einem ausgewählten verwalteten Gerät erkannt wurden, in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Liste der Schwachstellen in Programmen, die auf einem ausgewählten verwalteten Gerät erkannt wurden.

2. Wählen Sie die Schwachstellen in Programmen aus, die Sie exportieren möchten.

   Überspringen Sie diesen Schritt, wenn Sie eine vollständige Liste der auf dem verwalteten Gerät erkannten Schwachstellen in Programmen exportieren möchten.

   Wenn Sie eine vollständige Liste der auf dem verwalteten Gerät erkannten Schwachstellen in Programmen exportieren möchten, werden nur die auf der aktuellen Seite angezeigten Schwachstellen exportiert.

3. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format für den Export bevorzugt wird.

Die Datei mit der Liste der auf dem ausgewählten verwalteten Gerät erkannten Schwachstellen in Programmen wird auf das derzeit verwendete Gerät heruntergeladen.

Ignorieren von Schwachstellen in Programmen

Sie können Korrekturen für Software-Schwachstellen ignorieren. Gründe für das Ignorieren von Schwachstellen in Programmen können sein:

- Sie betrachten die Software-Schwachstelle nicht als kritisch für Ihr Unternehmen.
- Sie vermuten, dass durch das Schließen von Software-Schwachstellen die Daten des Programms beschädigt werden können, welches das Schließen von Schwachstellen erforderlich macht.
- Sie sind sicher, dass die Software-Schwachstelle keine Gefahr für das Netzwerk Ihres Unternehmens darstellt, da Sie andere Maßnahmen ergriffen haben, um Ihre verwalteten Geräte zu schützen.

Sie können eine Software-Schwachstelle auf allen verwalteten Geräten oder nur auf ausgewählten verwalteten Geräten ignorieren.

So ignorieren Sie eine Schwachstelle im Programm auf allen verwalteten Geräten:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Patch-Management → Schwachstellen in Programmen**.

   Auf der Seite wird die Liste der auf verwalteten Geräten erkannten Schwachstellen in Programmen angezeigt.

2. Klicken Sie in der Liste der Schwachstellen in Programmen auf den Link mit dem Namen der Schwachstelle, die Sie ignorieren möchten.

   Das Eigenschaftenfenster der Software-Schwachstelle wird geöffnet.

3. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Schwachstelle ignorieren**.

4. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Eigenschaftenfenster der Software-Schwachstelle wird geschlossen.

Die Schwachstelle im Programm wird auf allen verwalteten Geräten ignoriert.

Um eine Schwachstelle im Programm auf dem ausgewählten verwalteten Gerät zu ignorieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, auf dem Sie eine Software-Schwachstelle ignorieren möchten.

   Das Eigenschaftenfenster für das Gerät wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster des Geräts die Registerkarte **Erweitert** aus.

4. Wählen Sie im linken Bereich den Abschnitt **Schwachstellen in Programmen** aus.

   Die Liste der Software-Schwachstellen, die auf dem Gerät erkannt wurden, wird angezeigt.

5. Wählen Sie in der Liste der Software-Schwachstellen jene aus, die Sie auf dem ausgewählten Gerät ignorieren möchten.

   Das Fenster mit den Eigenschaften der Schwachstelle im Programm öffnet sich.

6. Aktivieren Sie im Eigenschaftenfenster der Schwachstelle im Programm auf der Registerkarte **Allgemein** die Option **Schwachstelle ignorieren**.

7. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Fenster mit den Eigenschaften der Schwachstelle im Programm schließt sich.

8. Schließen Sie das Eigenschaftenfenster des Geräts.

Die Software-Schwachstelle wird auf dem ausgewählten Gerät ignoriert.

Die ignorierte Software-Schwachstelle wird im Rahmen der Aufgabe *Schwachstellen schließen* oder *Erforderliche Updates installieren und Schwachstellen schließen* nicht behoben. Mithilfe eines Filters können Sie ignorierte Software-Schwachstellen aus der Liste der Schwachstellen ausschließen.

Verwalten des Programmstarts auf Client-Geräten

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center für die Verwaltung von Programmen beschrieben, die auf Client-Geräten installiert sind.

Programmkontrolle zur Verwaltung ausführbarer Dateien verwenden

Sie können die Programmkontrolle verwenden, um das Starten ausführbarer Dateien auf Benutzergeräten zu erlauben oder blockieren. Die Programmkontrolle unterstützt sowohl Windows- als auch Linux-basierte Betriebssysteme.

Für Linux-basierte Betriebssysteme ist die Programmkontrolle ab Kaspersky Endpoint Security 11.2 für Linux verfügbar. Darüber hinaus ist die Komponente für Kaspersky Embedded Systems Security für Windows ab Version 3.0 verfügbar.

Erforderliche Vorrausetzungen

- Kaspersky Security Center ist in Ihrer Organisation bereitgestellt.
- Die Richtlinie von Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security für Linux wurde erstellt und ist aktiv.
- Die Richtlinie von Kaspersky Embedded Systems Security für Windows oder Kaspersky Endpoint Security für Linux wurde erstellt und ist aktiv.

Schritte

Die Nutzung der Programmkontrolle erfolgt schrittweise:

1. **Erstellen und Anzeigen der Liste der ausführbaren Dateien auf Client-Geräten**

   Dieser Schritt unterstützt Sie dabei, herauszufinden, welche ausführbaren Dateien sich auf verwalteten Geräten befinden. Öffnen Sie die Liste der ausführbaren Dateien und vergleichen Sie diese mit den Listen der zulässigen und verbotenen ausführbaren Dateien. Die Einschränkungen zur Nutzung ausführbarer Dateien können sich auf die Informationssicherheitsrichtlinien des Unternehmens beziehen.

   Anleitung:

   - Verwaltungskonsole: Inventarisierung der ausführbaren Dateien
   - Kaspersky Security Center Web Console: Abrufen und Anzeigen einer Liste der auf Client-Geräten gespeicherten ausführbaren Dateien

2. **Erstellen von Kategorien für ausführbare Dateien, die in Ihrem Unternehmen verwendet werden**

   Analysieren Sie die Listen der ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind. Erstellen Sie basierend auf der Analyse Kategorien für ausführbare Dateien. Es wird empfohlen, die Kategorie "Arbeitsanwendung" zu erstellen, welche die Standardauswahl an ausführbaren Dateien enthält, die in Ihrem Unternehmen verwendet werden. Wenn von verschiedenen Sicherheitsgruppen unterschiedliche ausführbare Dateien verwendet werden, können Sie für jede Sicherheitsgruppe eine separate Kategorie erstellen.

   Anleitung:

   - Verwaltungskonsole: Manuell zu erweiternde Programmkategorie erstellen, Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen, Programmkategorie mit ausführbaren Dateien aus einem bestimmten Ordner erstellen.
   - Kaspersky Security Center Web Console: Manuell zu erweiternde Programmkategorie erstellen, Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen, Programmkategorie mit ausführbaren Dateien aus einem bestimmten Ordner erstellen.

3. **Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security**

   Konfigurieren Sie die Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security anhand der Kategorien, die Sie im vorherigen Schritt erstellt haben.

   Anleitung:

   - Verwaltungskonsole: Verwaltung des Programmstarts auf Client-Geräten anpassen
   - Kaspersky Security Center Web Console: Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows

4. **Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Embedded Systems Security**

Konfigurieren Sie die Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Embedded Systems Security für Windows anhand der Programmkategorien, die Sie bereits erstellt haben. Weitere Informationen über die Programmkontrolle finden Sie in der Hilfe zu Kaspersky Embedded Systems Security für Windows oder in der Hilfe zu Kaspersky Embedded Systems Security für Linux.

Wenn Sie eine große Anzahl an Regeln verwenden, kann beim Laden der Richtlinie ein Fehler auftreten. Sie können für die Anforderung die maximale Größe in Bytes mithilfe der folgenden Befehle erhöhen:

- Für die Anforderung mittels JSON:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
  ```

- Für die Anforderung mittels HTTP:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  Wobei `<max_request_size>` für die maximale Größe der Anforderung in Byte steht (z. B. `200000000`).

5. **Aktivieren der Komponente "Programmkontrolle" im Test-Modus**

   Um sicherzustellen, dass die Regeln der Programmkontrolle nicht die für die Benutzerarbeit erforderlichen ausführbaren Dateien blockieren, wird empfohlen, das Testen der Regeln der Programmkontrolle zu aktivieren und ihre Funktionsweise nach dem Erstellen neuer Regeln zu analysieren. Bei aktiviertem Test-Modus blockiert Kaspersky Embedded Systems Security für Windows keine ausführbaren Dateien, deren Start durch die Regeln der Programmkontrolle unzulässig ist. Stattdessen werden Benachrichtigungen über deren Start an den Administrationsserver gesendet.

   Es wird empfohlen, beim Testen von Regeln der Programmkontrolle die folgenden Aktionen auszuführen:

   - Festlegen des Testzeitraums. Der Testzeitraum kann zwischen mehreren Tagen und zwei Monaten liegen.
   - Untersuchen Sie die Ereignisse, die sich aus dem Testen der Funktionsweise der Programmkontrolle ergeben.

   Anleitung für Kaspersky Security Center Web Console: Konfigurieren der Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows. Folgen Sie dieser Anweisung und aktivieren Sie beim Konfigurieren die Option **Testbetrieb**.

6. **Ändern der Einstellungen für Kategorien der Komponente "Programmkontrolle"**

   Nehmen Sie bei Bedarf Änderungen an den Einstellungen für die Programmkontrolle vor. Auf der Grundlage der Testergebnisse können Sie einer zu erweiternden Kategorie manuell ausführbare Dateien hinzufügen, die sich auf Ereignisse der Programmkontrolle beziehen.

   Anleitung:

   - Verwaltungskonsole: Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen
   - Kaspersky Security Center Web Console: Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

7. **Anwenden der Regeln der Programmkontrolle im Funktionsmodus**

   Nachdem die Regeln der Programmkontrolle getestet wurden und die Konfiguration der Kategorien abgeschlossen ist, können Sie die Regeln der Programmkontrolle im Ausführungsmodus anwenden.

   Anleitung für Kaspersky Security Center Web Console: Konfigurieren der Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows. Folgen Sie dieser Anweisung und deaktivieren Sie beim Konfigurieren die Option **Testbetrieb**.

8. **Überprüfen der Konfiguration der Programmkontrolle**

Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

- Erstellen von Kategorien für ausführbare Dateien
- Konfigurieren der Programmkontrolle unter Verwendung der Kategorien
- Anwenden der Regeln der Programmkontrolle im Funktionsmodus

Ergebnisse

Wenn das Szenario abgeschlossen ist, wird der Start der ausführbaren Dateien auf den verwalteten Geräten gesteuert. Die Benutzer können nur jene ausführbaren Dateien starten, die in Ihrem Unternehmen erlaubt sind. Im Unternehmen verbotene ausführbare Dateien können nicht gestartet werden.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Modi und Kategorien der Programmkontrolle

Die Programmkontrolle überwacht die Versuche von Benutzern, ausführbare Dateien zu starten. Sie können Regeln der Programmkontrolle verwenden, um das Starten ausführbarer Dateien zu kontrollieren.

> Die Komponente "Programmkontrolle" ist für Kaspersky Endpoint Security für Windows, Kaspersky Endpoint Security 11.2 für Linux und höher und für Kaspersky Security for Virtualization Light Agent verfügbar. Alle Anleitungen in diesem Abschnitt beschreiben die Konfiguration der "Programmkontrolle" für Kaspersky Endpoint Security für Windows.

Das Starten von ausführbaren Dateien, deren Einstellungen keiner der Regeln der Programmkontrolle entsprechen, wird durch den ausgewählten Betriebsmodus der Komponente geregelt:

- *Deny-Liste*. Dieser Modus wird verwendet, wenn Sie den Start aller ausführbaren Dateien mit Ausnahme jener zulassen möchten, die in den Regeln zum Blockieren angegebenen sind. Dieser Modus ist standardmäßig festgelegt.
- *Allow-Liste*. Dieser Modus wird verwendet, wenn Sie den Start aller ausführbaren Programme mit Ausnahme jener blockieren möchten, die in den Regeln zum Zulassen angegeben sind.

Die Regeln der Programmkontrolle werden durch Kategorien implementiert, denen die ausführbaren Dateien zugeordnet werden. In Kaspersky Security Center gibt es drei Arten von Kategorien:

- Manuell zu erweiternde Kategorie. Sie definieren Bedingungen, z. B. Dateimetadaten, Datei-Hashcode, Dateizertifikat, KL-Kategorie oder Dateipfad, um ausführbare Dateien in die Kategorie aufzunehmen.
- Kategorie für ausführbare Dateien von ausgewählten Geräten. Sie geben ein Gerät an, dessen ausführbare Dateien automatisch in die Kategorie aufgenommen werden.
- Kategorie für ausführbare Dateien aus einem ausgewählten Ordner. Sie geben einen Ordner an, dessen ausführbare Dateien automatisch in die Kategorie aufgenommen werden.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen

Sie können die Liste der ausführbaren Dateien, die sich auf den Client-Geräten befinden, auf eine der folgenden Arten abrufen:

- Indem Sie in der Richtlinie von Kaspersky Endpoint Security die Benachrichtigungen über gestartete Anwendungen aktivieren.
- Indem Sie eine Inventarisierungsaufgabe erstellen.

In der Richtlinie von Kaspersky Endpoint Security die Benachrichtigungen über gestartete Anwendungen aktivieren

So aktivieren Sie die Benachrichtigungen über gestartete Anwendungen:

1. Öffnen Sie die Einstellungen der Richtlinie von Kaspersky Endpoint Security und wechseln Sie anschließend zu **Allgemeine Einstellungen → Berichte und Speicher**.
2. Aktivieren Sie in der Einstellungsgruppe **Datenübertragung an den Administrationsserver** das Kontrollkästchen **Über gestartete Anwendungen** und speichern Sie die Änderungen.

Wenn ein Benutzer versucht, ausführbare Dateien zu starten, werden Informationen über diese Dateien zur Liste der ausführbaren Dateien auf einem Client-Gerät hinzugefügt. Kaspersky Endpoint Security sendet diese Informationen an den Administrationsagenten, welcher sie anschließend an den Administrationsserver weiterleitet.

Eine Inventarisierungsaufgabe erstellen

Die Funktion zum Inventarisieren ausführbarer Dateien ist für die folgenden Programme verfügbar:

- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security für Linux ab Version 11.2
- Kaspersky Security for Virtualization 4.0 Light Agent und höhere Versionen

Sie können die Auslastung der Datenbank verringern und gleichzeitig Informationen über die installierten Anwendungen erhalten. Um Speicherplatz in der Datenbank zu sparen, führen Sie eine Inventarisierungsaufgabe auf Referenzgeräten durch, die mit Ihrem Software-Standardpaket ausgestattet sind. Die empfohlene Anzahl an Geräten beträgt 1-3.

Es wird dringend davon abgeraten, die Inventarisierungsaufgabe auszuführen, wenn Sie eine der folgenden Datenbanken verwenden: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (alle Editionen).

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.

   Die Aufgabenliste wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie auf der Seite **Einstellungen der neue Aufgabe** in der Dropdown-Liste **Programm** Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security für Linux, in Abhängigkeit des Betriebssystemtyps der Client-Geräte.

4. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Inventarisierung**.

5. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf **Fertigstellen**.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe **Inventarisierung** erstellt und angepasst. Wenn Sie möchten, können Sie die Einstellungen für die erstellte Aufgabe ändern. Daraufhin wird die neu erstellte Aufgabe in der Aufgabenliste angezeigt.

Weitere Informationen zur Inventarisierungsaufgabe finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent

Nach Ausführung der Aufgabe **Inventarisierung** wird die Liste der auf verwalteten Geräten gespeicherten ausführbaren Dateien erstellt und Sie können die Liste anzeigen.

Im Rahmen einer Inventarisierung können die Dateien folgender Formate erkannt werden (in Abhängigkeit Ihrer gewählten Optionen in den Aufgabeneigenschaften): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR und HTML.

Anzeigen der Liste mit ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind.

Um sich die Liste aller auf den Client-Geräten gespeicherten ausführbaren Dateien anzeigen zu lassen, gehen Sie wie folgt vor:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Ausführbare Dateien**.

Auf der Seite wird die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien angezeigt.

Bei Bedarf können Sie die ausführbare Datei des verwalteten Geräts an das Gerät senden, auf dem Ihre Kaspersky Security Center Web Console geöffnet ist.

So senden Sie eine ausführbare Datei:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Ausführbare Dateien**.
2. Klicken Sie auf den Link der ausführbaren Datei, die Sie senden möchten.
3. Wechseln Sie im nächsten Fenster zum Abschnitt **Geräte** und aktivieren Sie anschließend das Kontrollkästchen des verwalteten Geräts, von dem Sie die ausführbare Datei senden möchten.

   Stellen Sie vor dem Absenden der ausführbaren Datei durch das Aktivieren des Kontrollkästchens **Verbindung mit Administrationsserver nicht trennen** sicher, dass das verwaltete Gerät eine direkte Verbindung zum Administrationsserver besitzt.

4. Klicken Sie auf die Schaltfläche **Senden**.

   Die ausgewählte ausführbare Datei wird heruntergeladen, um sie anschließend an das Gerät mit Ihrer geöffneten Kaspersky Security Center Web Console weiterzusenden.

Erstellen einer manuell zu erweiternden Programmkategorie

Sie können einen Satz von Kriterien als Vorlage für ausführbare Dateien angeben, deren Start Sie in Ihrem Unternehmen zulassen oder blockieren möchten. Basierend auf ausführbaren Dateien, die den Kriterien entsprechen, können Sie eine Programmkategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

Um eine manuell zu erweiternde Programmkategorie zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programmkategorien**.

   Die Seite mit einer Liste der Programmkategorien wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie im Schritt **Methode zum Erstellen der Kategorie auswählen** des Assistenten die Option **Manuell zu erweiternde Kategorie. Daten über ausführbare Dateien werden manuell zur Kategorie hinzugefügt** aus.

4. Klicken Sie im Schritt **Bedingungen** des Assistenten auf **Hinzufügen**, um ein Bedingungskriterium für das Aufnehmen von Dateien in die Kategorie hinzuzufügen.

5. Wählen Sie im Schritt **Bedingungskriterien** einen Regeltyp zum Erstellen einer Kategorie aus der Liste aus:

   - **Aus der KL-Kategorie**

     Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Anwendungen in eine benutzerdefinierte Kategorie die Kategorie für Kaspersky-Anwendungen angeben. Programme, die zur angegebenen Kaspersky-Kategorie gehören, werden in die benutzerdefinierte Programmkategorie aufgenommen.

   - **Zertifikat aus Datenverwaltung auswählen**

     Wenn Sie diese Option auswählen, können Sie Zertifikate aus der Datenverwaltung angeben. Die Kategoriebedingung entspricht nur den ausführbaren Dateien, die durch das angegebene Zertifikat signiert sind.

     Zertifikate werden zur Datenverwaltung hinzugefügt, wenn Sie eine Inventarisierungsaufgabe erstellt und gestartet haben oder das Kontrollkästchen **Über ausgeführte Anwendungen in der Richtlinie von Kaspersky Endpoint Security** ausgewählt haben. Sie können beide Aktionen ausführen.

   - **Pfad des Programms festlegen (Masken unterstützt)**

     Wenn diese Option ausgewählt ist, können Sie den Pfad der Datei oder des Ordners auf dem Client-Gerät festlegen, der die ausführbaren Dateien enthält, die zur benutzerdefinierten Programmkategorie hinzugefügt werden sollen. Sie können reguläre Ausdrücke wie *C:\path_to_exe** verwenden, etwa: *C:\Programme\Internet Explorer**.

   - **Wechseldatenträger**

     Wenn Sie diese Variante wählen, können Sie einen Datenträgertyp (beliebiger oder Wechseldatenträger) angeben, auf dem die Anwendung ausgeführt wird. Die auf dem ausgewählten Datenträgertyp ausgeführten Anwendungen werden in die benutzerdefinierte Programmkategorie aufgenommen.

   - **Hash, Metadaten oder Zertifikat**:

     - **Aus Liste der ausführbaren Dateien auswählen**

       Wenn Sie diese Variante wählen, können Sie die Anwendungen, die in die Kategorie aufgenommen werden sollen, aus der Liste der ausführbaren Dateien des Client-Geräts auswählen.

- **Aus Programm-Registry auswählen**

  Wenn diese Option ausgewählt ist, wird die Programm-Registry angezeigt. Nachdem Sie eine Anwendung aus der Registrierung ausgewählt haben, öffnet sich ein Fenster mit den ausgefüllten Parametern der Metadaten für die ausgewählte Anwendung:

  - Dateiname.
  - Dateiversion. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
  - Name der Anwendung.
  - Version der Anwendung. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
  - Hersteller.

  Beachten Sie, dass nur der Start von ausführbaren Dateien, die den angegebenen Parametern entsprechen, blockiert wird, nicht aber der Start der ausgewählten Anwendung. Wenn die Metadaten der ausgewählten Anwendung mit denen der ausführbaren Datei übereinstimmen, die beim Anwendungsstart ausgeführt wird, können Sie mit dem nächsten Schritt fortfahren. Andernfalls müssen Sie die Werte manuell ändern, damit sie mit den Metadaten der ausführbaren Datei übereinstimmen.

- **Manuell angeben**

  Wenn Sie diese Option wählen, müssen Sie als Bedingung für die Aufnahme von Anwendungen in eine benutzerdefinierte Kategorie Datei-Hash, Metadaten oder Zertifikat angeben.

  Dateihash

  Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

  SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher unterstützt die Berechnung von SHA256. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows unterstützt.

Wählen Sie eine der Varianten zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center aus:

- Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheitsanwendungen dem Programm Kaspersky Endpoint Security 10 Service Pack 2 für Windows oder höher entsprechen, wählen Sie die das Kontrollkästchen **SHA256** aus. Es wird nicht empfohlen, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA256-Hash einer ausführbaren Datei" erstellt wurde. Das kann zum Absturz der Sicherheitsanwendungen führen. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion MD5 verwenden.

- Wenn in Ihrem Netzwerk niedrigere Versionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows installiert sind, wählen Sie die **MD5-Hash** aus. Für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows kann keine Kategorie hinzugefügt werden, die nach dem MD5-Prüfsummen-Kriterium der ausführbaren Datei erstellt wurde. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion SHA256 verwenden.

- Wenn verschiedene Geräte in Ihrem Netzwerk sowohl niedrigere als auch höhere Versionen von Kaspersky Endpoint Security 10 verwenden, aktivieren Sie die beiden Kontrollkästchen **SHA256** und **MD5-Hash**.

Metadaten

Wenn diese Option ausgewählt ist, können Sie Dateimetadaten als Dateinamen, Dateiversion und Hersteller angeben. Die Kategoriebedingung entspricht nur den ausführbaren Dateien mit denselben Metadaten.

Zertifikat

Wenn Sie diese Option auswählen, können Sie Zertifikate aus der Datenverwaltung angeben. Die Kategoriebedingung entspricht nur den ausführbaren Dateien, die durch das angegebene Zertifikat signiert sind.

Zertifikate werden zur Datenverwaltung hinzugefügt, wenn Sie eine Inventarisierungsaufgabe erstellt und gestartet haben oder das Kontrollkästchen **Über ausgeführte Anwendungen in der Richtlinie von Kaspersky Endpoint Security** ausgewählt haben. Sie können beide Aktionen ausführen.

- **Aus der Datei oder aus dem MSI-Paket/archiviertem Ordner**

  Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie eine MSI-Installationsdatei angeben. Die Metadaten des Installers werden an den Administrationsserver weitergegeben. Programme, deren Installer-Metadaten mit denen des MSI-Installers übereinstimmen, werden in die benutzerdefinierte Programmkategorie aufgenommen.

Das ausgewählte Kriterium wird zur Liste mit Kriterien hinzugefügt.

Sie können so viele Kriterien in die erstellende Programmkategorie aufnehmen, wie Sie benötigen.

6. Klicken Sie in dem Schritt **Ausschlüsse** auf **Hinzufügen**, um ein exklusives Bedingungskriterium hinzufügen, nach dem Dateien aus der gerade erstellten Kategorie ausgeschlossen werden sollen.

7. Wählen Sie im Schritt **Bedingungskriterien** einen Regeltyp aus der Liste aus, so wie Sie einen Regeltyp zum Erstellen einer Kategorie ausgewählt haben.

Nach Abschluss des Assistenten wird die Programmkategorie erstellt. Sie wird in der Liste der Programmkategorien angezeigt. Sie können die erstellte Programmkategorie verwenden, wenn Sie die "Programmkontrolle" anpassen.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen

Sie können ausführbare Dateien von ausgewählten Geräten als Vorlage für ausführbare Dateien verwenden, die Sie zulassen oder blockieren möchten. Basierend auf ausführbaren Dateien von ausgewählten Geräten können Sie eine Kategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

So rufen Sie die Liste der ausführbaren Dateien von Geräten ab:

1. Stellen Sie sicher, dass die Richtlinie von Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security für Linux erstellt wurde und aktiv ist. Aktivieren Sie in der Richtlinie die Komponente "Programmkontrolle".
2. Rufen Sie die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien ab.

Um eine Kategorie zu erstellen, die ausführbare Dateien von ausgewählten Geräten enthält, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programmkategorien**.

   Die Seite mit der Liste an Kategorien wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.
3. Geben Sie in dem Schritt **Methode zum Erstellen der Kategorie auswählen** den Kategorienamen ein und wählen Sie die Option **Kategorie für ausführbare Dateien von ausgewählten Geräten. Diese ausführbaren Dateien werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.
5. Wählen Sie im folgenden Fenster ein Gerät oder mehrere Geräte aus, deren ausführbare Dateien zum Erstellen der Kategorie verwendet werden sollen.
6. Geben Sie die folgenden Einstellungen an:

   - **Algorithmus für die Berechnung der Hash-Funktion**

     Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher unterstützt die Berechnung von SHA256. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows unterstützt.

Wählen Sie eine der Varianten zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center aus:

- Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheitsanwendungen dem Programm Kaspersky Endpoint Security 10 Service Pack 2 für Windows oder höher entsprechen, wählen Sie die das Kontrollkästchen **SHA256** aus. Es wird nicht empfohlen, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA256-Hash einer ausführbaren Datei" erstellt wurde. Das kann zum Absturz der Sicherheitsanwendungen führen. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion MD5 verwenden.

- Wenn in Ihrem Netzwerk niedrigere Versionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows installiert sind, wählen Sie die **MD5-Hash** aus. Für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows kann keine Kategorie hinzugefügt werden, die nach dem MD5-Prüfsummen-Kriterium der ausführbaren Datei erstellt wurde. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion SHA256 verwenden.

Wenn verschiedene Geräte in Ihrem Netzwerk sowohl niedrigere als auch höhere Versionen von Kaspersky Endpoint Security 10 verwenden, aktivieren Sie die beiden Kontrollkästchen **SHA256** und **MD5-Hash**.

Standardmäßig ist das Kontrollkästchen **SHA256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)** aktiviert.

Standardmäßig ist das Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)** deaktiviert.

- **Daten mit der Datenverwaltung des Administrationsservers synchronisieren**

  Wählen Sie diese Option, wenn der Administrationsserver die Änderungen in dem bzw. den angegebenen Ordner(n) regelmäßig überprüfen soll.

  Diese Option ist standardmäßig deaktiviert.

  Wenn Sie diese Option aktivieren, geben Sie den Zeitraum (in Stunden) an, in dem die Änderungen in den angegebenen Ordnern überprüft werden sollen. Standardmäßig beträgt das Untersuchungsintervall 24 Stunden.

- **Dateityp**

  In diesem Abschnitt können Sie den Dateityp angeben, mit dem die Programmkategorie erstellt wird.

  Alle Dateien. Alle Dateien werden beim Erstellen der Kategorie berücksichtigt. Diese Variante ist standardmäßig ausgewählt.

  Nur Dateien, die keiner Programmkategorie entsprechen. Nur Dateien außerhalb der Programmkategorien werden beim Erstellen der Kategorie berücksichtigt.

- **Ordner**

  In diesem Abschnitt können Sie Ordner auf dem ausgewählten Gerät (bzw. den ausgewählten Geräten) angeben, die Dateien enthalten, mit denen die Programmkategorie erstellt wird.

  Alle Ordner. Alle Ordner werden beim Erstellen der Kategorie berücksichtigt. Diese Variante ist standardmäßig ausgewählt.

Angegebener Ordner. Nur der angegebene Ordner wird beim Erstellen der Kategorie berücksichtigt. Bei Auswahl dieser Option müssen Sie den Pfad zum Ordner angeben.

Nach Abschluss des Assistenten wird die Kategorie für ausführbare Dateien erstellt. Sie wird in der Liste der Kategorien angezeigt. Sie können die erstellte Kategorie verwenden, wenn Sie die Programmkontrolle konfigurieren.

Erstellen einer Programmkategorie mit ausführbaren Dateien aus einem ausgewählten Ordner

Sie können die ausführbaren Dateien aus einem bestimmten Ordner als Standard für die ausführbaren Dateien verwenden, die Sie in Ihrem Unternehmen zulassen oder blockieren möchten. Basierend auf den ausführbaren Dateien aus dem ausgewählten Ordner können Sie eine Programmkategorie erstellen und diese verwenden, um die Komponente "Programmkontrolle" anzupassen.

Um eine Kategorie zu erstellen, die ausführbare Dateien aus dem ausgewählten Ordner enthält:

1. Gehen Sie im Hauptmenü zu **Vorgänge → Drittanbieter-Programme → Programmkategorien**.

   Die Seite mit der Liste an Kategorien wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

3. Geben Sie im Schritt **Methode zum Erstellen der Kategorie auswählen** den Kategorienamen ein und wählen Sie die Option **Kategorie für ausführbare Dateien aus einem bestimmten Ordner. Ausführbare Dateien von Programmen, die sich in dem angegebenen Ordner befinden, werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt** aus.

4. Geben Sie den Ordner an, dessen ausführbare Dateien zum Erstellen der Kategorie verwendet werden.

5. Passen Sie die folgenden Einstellungen an:

   - **Dynamic Link Libraries (.dll) in diese Kategorie aufnehmen**

     Zur Programmkategorie werden dynamisch verbundene Bibliotheken (dll-Dateien) hinzugefügt und die Komponente "Programmkontrolle" registriert die Aktionen solcher Bibliotheken, die im System gestartet werden. Es ist möglich, dass nach der Aufnahme von dll-Dateien in die Kategorie die Leistung von Kaspersky Security Center sinkt.

     Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

   - **Skriptdateien in diese Kategorie aufnehmen**

     Zur Programmkategorie werden Informationen zu Skripten hinzugefügt und die Skripte werden von der Komponente "Schutz vor Web-Bedrohungen" nicht gesperrt. Es ist möglich, dass nach der Aufnahme von Daten zu Skripten in die Kategorie die Leistung von Kaspersky Security Center sinkt.

     Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Algorithmus für die Berechnung der Hash-Funktion**: **SHA256 für die Dateien der Kategorie berechnen (unterstützt von Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher) / MD5 für die Dateien der Kategorie berechnen (unterstützt von Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**

  Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

  SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher unterstützt die Berechnung von SHA256. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows unterstützt.

  Wählen Sie eine der Varianten zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center aus:

  - Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheitsanwendungen dem Programm Kaspersky Endpoint Security 10 Service Pack 2 für Windows oder höher entsprechen, wählen Sie die das Kontrollkästchen **SHA256** aus. Es wird nicht empfohlen, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA256-Hash einer ausführbaren Datei" erstellt wurde. Das kann zum Absturz der Sicherheitsanwendungen führen. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion MD5 verwenden.

  - Wenn in Ihrem Netzwerk niedrigere Versionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows installiert sind, wählen Sie die **MD5-Hash** aus. Für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows kann keine Kategorie hinzugefügt werden, die nach dem MD5-Prüfsummen-Kriterium der ausführbaren Datei erstellt wurde. In diesem Fall können Sie für Dateien der Kategorie die kryptografische Hash-Funktion SHA256 verwenden.

  Wenn verschiedene Geräte in Ihrem Netzwerk sowohl niedrigere als auch höhere Versionen von Kaspersky Endpoint Security 10 verwenden, aktivieren Sie die beiden Kontrollkästchen **SHA256** und **MD5-Hash**.

  Standardmäßig ist das Kontrollkästchen **SHA256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)** aktiviert.

  Standardmäßig ist das Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)** deaktiviert.

- **Untersuchung des Ordners auf Änderungen erzwingen**

  Wenn diese Option aktiviert ist, erzwingt das Programm regelmäßig eine Prüfung des Ordners für die Erweiterung von Kategorien auf Veränderungen. Das Prüfintervall in Stunden kann im Eingabefeld neben dem Kontrollkästchen eingegeben werden. Standardmäßig beträgt das Intervall für die erzwungene Prüfung 24 Stunden.

  Ist diese Option deaktiviert, erfolgt keine erzwungene Prüfung des Ordners. Der Server greift auf die Dateien im Ordner zu, wenn diese verändert, hinzugefügt oder gelöscht werden.

  Diese Option ist standardmäßig deaktiviert.

Nach Abschluss des Assistenten wird die Kategorie der ausführbaren Dateien erstellt. Sie wird in der Liste der Kategorien angezeigt. Sie können die Kategorie in der Konfiguration der Programmkontrolle verwenden.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux

- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Liste der Programmkategorien anzeigen

Sie können die Liste der konfigurierten Kategorien für die ausführbaren Dateien und die Einstellungen der einzelnen Kategorien anzeigen.

Um die Liste der Programmkategorien anzuzeigen,

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programmkategorien**.

Die Seite mit der Liste an Kategorien wird angezeigt.

Um die Eigenschaften einer Programmkategorie anzuzeigen,

Klicken Sie auf den Namen der Kategorie.

Das Eigenschaftenfenster der Kategorie wird angezeigt. Die Eigenschaften sind auf mehreren Registerkarten angeordnet.

Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

Nachdem Sie die "Programmkontrolle" in den Richtlinien von Kaspersky Endpoint Security für Windows angepasst haben, werden in der Ereignisliste die folgenden Ereignisse angezeigt:

- **Programmstart verboten** (*kritisches* Ereignis). Dieses Ereignis wird angezeigt, wenn Sie die Programmkontrolle so konfiguriert haben, dass Regeln angewendet werden.
- **Der Start der Anwendung ist im Testbetrieb untersagt** (*Infomeldungsereignis*). Dieses Ereignis wird angezeigt, wenn Sie die Programmkontrolle so konfiguriert haben, dass Regeln getestet werden.
- **Nachricht an den Administrator über verbotene Programmstarts** (Ereignistyp *Warnung*). Dieses Ereignis wird angezeigt, wenn Sie in der "Programmkontrolle" das Anwenden von Regeln festgelegt haben, und ein Benutzer auf eine Anwendung zugreifen möchte, das beim Start blockiert wurde.

Es wird empfohlen, Ereignisauswahlen zu erstellen, um Ereignisse anzuzeigen, die sich auf den Betrieb der Programmkontrolle beziehen.

Sie können ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu einer vorhandenen Programmkategorie oder zu einer neuen Programmkategorie hinzufügen. Das Hinzufügen ausführbarer Dateien ist jedoch nur bei einer manuell zu erweiternden Programmkategorie möglich.

Um ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu einer Programmkategorie hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.

   Die Liste der Ereignisauswahlen wird angezeigt.

2. Wählen Sie die Ereignisauswahl aus, um Ereignisse im Zusammenhang mit der Programmkontrolle anzuzeigen und diese Ereignisauswahl zu starten.

   Wenn Sie keine Ereignisauswahl für die Programmkontrolle erstellt haben, können Sie eine vordefinierte Auswahl auswählen und starten, z. B. **Letzte Ereignisse**.

   Die Liste der Ereignisse wird angezeigt.

3. Wählen Sie die Ereignisse aus, für die Sie ausführbare Dateien der Programmkategorie hinzufügen möchten, und klicken Sie auf **Einer Kategorie zuweisen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

4. Legen Sie auf der Seite des Assistenten die relevanten Einstellungen fest:

   - Wählen Sie im Abschnitt **Aktion mit der zum Ereignis gehörenden ausführbaren Datei** eine der folgenden Optionen aus:

     - **Zu neuer Programmkategorie hinzufügen**

       Wählen Sie diese Option, wenn Sie eine neue Programmkategorie basierend auf ereignisbezogenen ausführbaren Dateien erstellen möchten.

       Diese Variante ist standardmäßig ausgewählt.

       Wenn Sie diese Option ausgewählt haben, geben Sie einen neuen Kategorienamen an.

     - **Zu bestehender Programmkategorie hinzufügen**

       Wählen Sie diese Option, wenn Sie in einer bestehenden Programmkategorie ereignisbezogene ausführbare Dateien hinzufügen möchten.

       Diese Variante ist standardmäßig nicht ausgewählt.

       Wenn Sie diese Option ausgewählt haben, wählen Sie die Programmkategorie mit manuell hinzugefügtem Inhalt aus, zu der Sie ausführbare Dateien hinzufügen möchten.

   - Wählen Sie im Abschnitt **Regeltyp** eine der folgenden Optionen aus:

     - **Regeln zum Hinzufügen zu den Einschlüssen**

     - **Regeln zum Hinzufügen zu den Ausschlüssen**

   - Wählen Sie im Abschnitt **Als Bedingung verwendete Parameter** eine der folgenden Optionen aus:

     - **Zertifikatdaten (oder SHA256-Hashs für Dateien ohne ein Zertifikat)**

       Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen einer Anwendung von einem Zertifikat signiert sein oder mehrere verschiedene Anwendungen eines Herstellers können von einem Zertifikat signiert sein. Bei der Wahl des Zertifikates können mehrere Anwendungsversionen oder mehrere Anwendungen eines Herstellers in der Kategorie vorhanden sein.

       Jede Datei hat ihre eindeutige SHA256-Hash-Funktion. Bei der Auswahl der SHA256-Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Anwendungsversion.

       Wählen Sie diese Variante, wenn Sie die die Zertifikatsdetails einer ausführbaren Datei (oder die SHA256-Hash-Funktion für Dateien ohne Zertifikat) zu den Regeln der Kategorie hinzufügen möchten.

       Diese Variante ist standardmäßig ausgewählt.

- **Zertifikatdaten (Dateien ohne ein Zertifikat werden übersprungen)**

  Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen einer Anwendung von einem Zertifikat signiert sein oder mehrere verschiedene Anwendungen eines Herstellers können von einem Zertifikat signiert sein. Bei der Wahl des Zertifikates können mehrere Programmversionen oder mehrere Programme eines Herstellers in der Kategorie vorhanden sein.

  Wählen Sie diese Variante, wenn Sie die Zertifikatsdaten einer ausführbaren Datei zu den Regeln der Kategorie hinzufügen möchten. Wenn die ausführbare Datei kein Zertifikat hat, wird eine solche Datei übersprungen. Die entsprechenden Informationen werden nicht zur Kategorie hinzugefügt.

- **Nur SHA256 (Dateien ohne Hash werden übersprungen)**

  Jede Datei hat ihre eindeutige SHA256-Hash-Funktion. Bei der Auswahl der SHA256-Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Programmversion.

  Wählen Sie diese Variante, wenn Sie nur die Daten der SHA256-Hash-Funktion einer ausführbaren Datei zu den Regeln der Kategorie hinzufügen möchten

- **Nur MD5 (Modus eingestellt; Nur für die Version Kaspersky Endpoint Security 10 Service Pack 1)**

  Jede Datei hat ihre eindeutige MD5 Hash-Funktion. Bei der Auswahl der MD5 Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Anwendungsversion.

  Wählen Sie diese Variante, wenn Sie nur die Details der MD5-Hash-Funktion einer ausführbaren Datei hinzufügen möchten. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 1 für Windows unterstützt.

5. Klicken Sie auf die Schaltfläche **OK**.

Nach Abschluss des Assistenten werden ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu der vorhandenen Programmkategorie oder zu einer neuen Programmkategorie hinzugefügt. Sie können die Einstellungen der Programmkategorie anzeigen, die Sie geändert oder erstellt haben.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows konfigurieren

Nachdem Sie die Kategorien der Programmkontrolle erstellt haben, können Sie diese verwenden, um die Programmkontrolle in den Richtlinien von Kaspersky Endpoint Security für Windows anzupassen.

So konfigurieren Sie die Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

   Eine Seite mit einer Liste der Richtlinien wird angezeigt.

2. Klicken Sie auf die Richtlinie **Kaspersky Endpoint Security für Windows**.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.

3. Wechseln Sie zu **Programmeinstellungen → Sicherheitskontrollen → Programmkontrolle**.

   Das Fenster **Programmkontrolle** wird mit den entsprechenden Eigenschaften angezeigt.

4. Die Option **Programmkontrolle** ist standardmäßig aktiviert. Stellen Sie sicher, dass die Umschalttaste **Programmkontrolle DEAKTIVIERT** auf die deaktivierte Position gesetzt ist.

5. Aktiveren Sie in den Sperreinstellungen der **Einstellungen der Programmkontrolle** den Ausführungsmodus, um die Regeln der Programmkontrolle anzuwenden und Kaspersky Endpoint Security für Windows zu erlauben, den Start von Programmen zu blockieren.

   Wenn Sie die Regeln der Programmkontrolle testen möchten, können Sie in den **Einstellungen der Programmkontrolle** den Testmodus aktivieren. Im Testmodus blockiert Kaspersky Endpoint Security für Windows den Start von Programmen nicht, sondern protokolliert Informationen über ausgelöste Regeln im Bericht. Klicken Sie auf den Link **Bericht anzeigen**, um diese Informationen anzuzeigen.

6. Aktivieren Sie die Option **Laden von DDL-Modulen überwachen**, wenn Kaspersky Endpoint Security für Windows beim Starten von Anwendungen das Laden von DLL-Modulen überwachen soll.

   Informationen über das Modul und die Anwendung, die das Modul geladen hat, werden in einem Bericht gespeichert.

   Kaspersky Endpoint Security für Windows überwacht nur die DLL-Module und -Treiber, die nach der Auswahl der Option **Laden von DDL-Modulen überwachen** geladen wurden. Starten Sie das Gerät nach Auswahl der Option **Laden von DLL-Modulen überwachen** neu, wenn Kaspersky Endpoint Security für Windows alle DLL-Module und -Treiber überwachen soll. Dies betrifft auch jene, die vor dem Start von Kaspersky Endpoint Security für Windows geladenen werden.

7. (Optional) Ändern Sie im Block **Nachrichtenvorlagen** die Vorlage der Nachricht, die bei einer Blockierung eines Anwendungsstarts angezeigt wird, sowie die Vorlage der E-Mail, die an Sie gesendet wird.

8. Wählen Sie im Einstellungsblock **Modus der Programmkontrolle** den Modus **Deny-Liste** oder **Allow-Liste** aus.

   Der Modus **Deny-Liste** ist standardmäßig ausgewählt.

9. Klicken Sie auf den Link **Einstellungen für Regellisten**.

   Das Fenster **Deny-Listen und Allow-Listen** wird geöffnet. Dort können Sie eine Programmkategorie hinzufügen. Standardmäßig ist die Registerkarte **Deny-Liste** ausgewählt, wenn der Modus **Deny-Liste** ausgewählt ist, bzw. die Registerkarte **Allow-Liste**, wenn der Modus **Allow-Liste** ausgewählt ist.

10. Klicken Sie im Fenster **Deny-Listen und Allow-Listen** auf **Hinzufügen**.

    Das Fenster **Regel der Programmkontrolle** wird geöffnet.

11. Klicken Sie auf den Link **Bitte wählen Sie eine Kategorie**.

    Das Fenster **Programmkategorie** wird geöffnet.

12. Fügen Sie die zuvor erstellte Programmkategorie(n) hinzu.

    Klicken Sie auf **Bearbeiten**, um die Einstellungen einer erstellten Kategorie zu bearbeiten.

    Klicken Sie auf **Hinzufügen**, um eine neue Kategorie zu erstellen.

    Klicken Sie auf **Löschen**, um eine Kategorie aus der Liste zu löschen.

13. Nachdem Sie die Liste der Programmkategorien erstellt haben, klicken Sie auf **OK**.

    Das Fenster **Programmkategorie** wird geschlossen.

14. Erstellen Sie im Fenster der Regel der **Programmkontrolle** im Abschnitt **Subjekte und deren Rechte** eine Liste der Benutzer und Benutzergruppen, für welche die Regel der Programmkontrolle gelten soll.

15. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster **Regel der Programmkontrolle** zu schließen.

16. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster **Deny-Listen und Allow-Listen** zu schließen.

17. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster **Programmkontrolle** zu schließen.

18. Schließen Sie das Fenster mit den Richtlinieneinstellungen für Kaspersky Endpoint Security für Windows.

    Die Programmkontrolle wird konfiguriert. Nachdem die Richtlinie an die Client-Geräte verteilt wurde, wird der Start der ausführbaren Dateien verwaltet.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Aufrufen und Anzeigen einer Liste der auf Client-Geräten installierten Programme

Kaspersky Security Center führt eine Inventarisierung der Software durch, die auf den verwalteten Client-Geräten unter Linux und Windows installiert ist.

Der Administrationsagent erstellt eine Liste der auf dem Gerät installierten Programme und leitet die Liste an den Administrationsserver weiter. Es dauert etwa 10-15 Minuten, bis der Administrationsagent die Anwendungsliste aktualisiert hat.

Bei Windows-basierten Client-Geräten erhält der Administrationsagent die meisten Informationen über installierte Anwendungen aus der Windows-Registrierung. Bei Linux-basierten Client-Geräten werden dem Administrationsagenten die Informationen über installierte Anwendungen durch die Paketmanager bereitgestellt.

> Wenn eine Anwendung aus dem Abschnitt **Programm-Registry** auf einem Linux-Gerät gefunden wurde, enthalten die Anwendungseigenschaften keine Informationen über zugehörige ausführbare Dateien.

Um die Liste mit auf verwalteten Geräten installierten Anwendungen anzuzeigen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.

   Die Seite zeigt eine Tabelle mit den Programmen an, die auf verwalteten Geräten installiert sind. Wählen Sie ein Programm aus, um seine Eigenschaften anzeigen, z. B. Name des Anbieters, Versionsnummer, Liste der ausführbaren Dateien, Liste mit Geräten mit dem installierten Programm, Liste mit verfügbaren Programm-Updates und Liste mit gefundenen Schwachstellen in Programmen.

2. Sie können die Daten der Tabelle mit installierten Programmen wie folgt gruppieren und filtern:

   - Klicken Sie auf das Einstellungen-Symbol ( ) in der oberen rechten Ecke der Tabelle.

     Wählen Sie im geöffneten Menü **Spalten-Einstellungen** die Spalten aus, die in der Tabelle angezeigt werden sollen. Um den Betriebssystemtyp der Client-Geräte anzuzeigen, auf denen die Anwendung installiert ist, wählen Sie die Spalte **Typ des Betriebssystems** aus.

   - Klicken Sie auf das Filter-Symbol ( ) in der oberen rechten Ecke der Tabelle, geben Sie anschließend das Filterkriterium im aufgerufenen Menü an und wenden Sie es an.

     Die gefilterte Tabelle der installierten Anwendungen wird angezeigt.

So zeigen Sie eine Liste der Anwendungen an, die auf bestimmten verwalteten Geräten installiert sind:

Gehen Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte** → **<Gerätename>** → **Erweitert** → **Programm-Registry**. In diesem Menü können Sie die Liste der Programme als csv- oder txt-Datei exportieren.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux
- Kaspersky Security for Virtualization Light Agent
- Hilfe von Kaspersky Embedded Systems Security für Windows
- Hilfe von Kaspersky Embedded Systems Security für Linux

Erstellen eines Installationspakets eines Drittanbieterprogramms aus der Kaspersky-Datenbank

Mit Kaspersky Security Center Web Console können Sie mithilfe von Installationspaketen eine Remote-Installation von Drittanbieterprogrammen durchführen. Solche Drittanbieterprogramme sind in einer dedizierten Kaspersky-Datenbank enthalten. Diese Datenbank wird automatisch erstellt, wenn Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* starten.

So erstellen Sie ein Installationspaket eines Drittanbieterprogramms aus der Kaspersky-Datenbank:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Wählen Sie auf der Seite "Assistent für das Erstellen eines Installationspakets" die Option **Installationspaket für ein ausgewähltes Programm aus der Kaspersky-Datenbank erstellen** und klicken Sie anschließend auf **Weiter**.

4. Wählen Sie in der nun geöffneten Liste der Programme das entsprechende Programm aus und klicken Sie anschließend auf **Weiter**.

5. Wählen Sie die entsprechende Lokalisierungssprache in der Dropdown-Liste aus und klicken Sie anschließend auf **Weiter**.

   Dieser Schritt wird nur angezeigt, wenn die Anwendung mehrere Sprachoptionen zur Auswahl bietet.

6. Wenn Sie aufgefordert werden, einen Lizenzvertrag für die Installation zu akzeptieren, können Sie auf der nun geöffneten **Endbenutzer-Lizenzvertrag**-Seite auf den Link klicken, um den Lizenzvertrag auf der Website des Anbieters zu lesen. Aktivieren Sie dann das Kontrollkästchen **Ich bestätige, dass ich die Bestimmungen und Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe und sie verstehe und akzeptiere**.

7. Auf der nun geöffneten **Name des neuen Installationspakets**-Seite geben Sie im Feld **Paketname** den Namen für das Installationspaket ein und klicken anschließend auf **Weiter**.

Warten Sie, bis das neu erstellte Installationspaket auf den Administrationsserver hochgeladen wurde. Wenn Ihnen vom Assistenten für das Erstellen eines Installationspakets die Nachricht angezeigt wird, dass der Prozess der Paketerstellung erfolgreich war, klicken Sie auf **Fertigstellen**.

Das erstellte Installationspaket wird in der Liste der Installationspakete aufgeführt. Sie können dieses Paket auswählen, wenn Sie die Aufgabe *Remote-Installation des Programms* erstellen oder neukonfigurieren.

Anzeigen und anpassen der Einstellungen von einem Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank

Wenn Sie bereits Installationspakete für Drittanbieter-Anwendungen erstellt haben, die in der Kaspersky-Datenbank gelistet sind, können Sie die Einstellungen dieser Pakete später anzeigen und anpassen.

Das Anpassen der Einstellungen eines Installationspakets eines Drittanbieter-Programms steht nur unter der Lizenz für das Schwachstellen- und Patch-Management zur Verfügung.

Um die Einstelllungen eines Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank anzuzeigen und anzupassen:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.

2. Klicken Sie in der Liste der Installationspakete auf den Namen des benötigten Installationspakets.

3. Passen Sie bei Bedarf auf der sich öffnenden Seite mit den Eigenschaften des Pakets die Einstellungen an.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die geänderten Einstellungen werden gespeichert.

Einstellungen eines Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank

Die Einstellungen für das Installationspaket eines Drittanbieter-Programms sind auf den folgenden Registerkarten gruppiert:

Von den unten aufgeführten Einstellungen wird standardmäßig nur ein Teil angezeigt. Sie können die entsprechenden Spalten durch anklicken der Schaltfläche **Filter** und auswählen der benötigten Spaltennamen aus der Liste hinzufügen.

- Registerkarte **Allgemein**:
  - Eingabefeld, welches den Namen des Installationspakets enthält und manuell bearbeitet werden kann
  - **Programm**

    Name der Drittanbieter-Anwendung, für welche das Installationspaket erstellt wurde.
  - **Version**

    Versionsnummer der Drittanbieter-Anwendung, für welche das Installationspaket erstellt wurde.
  - **Größe**

    Größe des Drittanbieter-Installationspakets (in Kilobyte).
  - **Erstellt**

    Datum und Uhrzeit der Erstellung des Drittanbieter-Installationspakets.
  - **Pfad**

    Pfad des Netzwerkordners, in dem sich das Drittanbieter-Installationspaket befindet.
- Registerkarte **Installationsreihenfolge**:
  - **Erforderliche allgemeine Systemkomponenten installieren**

    Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

    Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

    Diese Option ist standardmäßig deaktiviert.
  - Eine Tabelle, welche die Update-Eigenschaften anzeigt, und über folgende Spalten verfügt:
    - **Name**

      Name des Updates.

- **Beschreibung**

  Beschreibung des Updates.

- **Quelle**

  Quelle des Updates, d. h. ob das Update von Microsoft oder von einem anderen Drittanbieter veröffentlicht wurde.

- **Typ**

  Typ des Updates, d. h. ob es für einen Treiber oder für ein Programm vorgesehen ist.

- **Kategorie**

  Die für Microsoft-Updates angegebene Kategorie des Windows Server Update-Dienstes (WSUS) (Kritische Updates, Definitions-Updates, Treiber, Funktionspakete, Sicherheits-Updates, Service Packs, Tools, Update-Rollups, Updates oder Upgrades).

- **Ereigniskategorie nach MSRC**

  Die durch das Microsoft Security Response Center (MSRC) definierte Ereigniskategorie des Updates.

- **Ereigniskategorie**

  Die durch Kaspersky definierte Ereigniskategorie des Updates.

- **Ereigniskategorie des Patches**

  Ereigniskategorie eines Patches, wenn dieser für eine Kaspersky-Anwendung vorgesehen ist.

- **Artikel**

  ID des Artikels, der das Update in der Wissensdatenbank beschreibt.

- **Bulletin**

  ID des Sicherheitsbulletins mit einer Beschreibung des Updates.

- **Nicht zur Installation bestimmt (neue Version)**

  Gibt an, ob das Update den Status "Nicht zur Installation bestimmt" besitzt.

- **Bestimmt für die Installation**

  Gibt an, ob das Update den Status "Für die Installation bestimmt" besitzt.

- **Wird installiert**

  Gibt an, ob das Update den Status "Wird installiert" besitzt.

- **Installiert**

  Gibt an, ob das Update den Status "Installiert" besitzt.

- **Fehlgeschlagen**

  Gibt an, ob das Update den Status "Fehlgeschlagen" besitzt.

- **Neustart erforderlich**

  Gibt an, ob das Update den Status "Neustart erforderlich" besitzt.

- **Registriert**

  Gibt den Zeitpunkt (Datum und Uhrzeit) an, zu dem das Update registriert wurde.

- **Wird im interaktiven Modus installiert**

  Gibt an, ob das Update während der Installation Benutzerinterkation erfordert.

- **Zurückgerufen**

  Gibt Datum und Uhrzeit an, wann das Update widerrufen wurde.

- **Status der Update-Genehmigung**

  Gibt an, ob das Update zur Installation genehmigt wurde.

- **Revision**

  Gibt die aktuelle Revisionsnummer des Updates an.

- **Update-ID**

  Gibt die Update-ID an.

- **Programmversion**

  Gibt die Versionsnummer an, auf die das Programm aktualisiert wird.

- **Ersetzt**

  Gibt ein oder mehrere andere Updates an, die dieses Update ersetzen können.

- **Ersetzend**

  Gibt ein oder mehrere Updates an, die durch dieses Update ersetzt werden können.

- **Sie müssen die Bedingungen des Lizenzvertrags akzeptieren**

  Gibt an, ob das Update das Akzeptieren des Endbenutzer-Lizenzvertrags (EULA) erfordert.

- **URL der Beschreibung**

  Gibt den Namen des Update-Herstellers an.

- **Programmfamilie**

  Gibt den Namen der Programmfamilie an, zu welcher dieses Update gehört.

- **Programm**

  Gibt den Namen des Programms an, zu dem dieses Update gehört.

- **Lokalisierungssprache**

  Gibt die Sprache der Update-Lokalisierung an.

- **Nicht zur Installation bestimmt (neue Version)**

  Gibt an, ob das Update den Status "Nicht zur Installation bestimmt (neue Version)" besitzt.

- **Erforderliche Komponenten müssen installiert werden**

  Gibt an, ob das Update den Status "Erforderliche Komponenten müssen installiert werden" besitzt.

- **Download-Modus**

  Gibt den Modus des Update-Downloads an.

- **Ist ein Patch**

  Gibt an, ob das Update ein Patch ist.

- **Nicht installiert**

  Gibt an, ob das Update den Status "Nicht installiert" besitzt.

- Registerkarte **Einstellungen** welche die Einstellungen des Installationspakets – mit ihren Namen, Beschreibungen und Werten – anzeigt, die als Befehlszeilenparameter während der Installation verwendet werden. Wenn ein Paket nicht über derartige Einstellungen verfügt, wird ein entsprechender Hinweis angezeigt. Die Werte dieser Einstellungen können angepasst werden.

- Registerkarte **Revisionsverlauf**, welche die Revisionen des Installationspakets anzeigt und über folgende Spalten verfügt:

  - **Revision** – Revisionsnummer des Installationspakets
  - **Uhrzeit** – Datum und Uhrzeit der Änderung der Einstellungen des Installationspakets
  - **Benutzer** – Name des Benutzers, der die Einstellungen des Installationspakets geändert hat
  - **Aktion** – Aktion, die am Installationspaket während der Revision durchgeführt wurden
  - **Beschreibung** – Beschreibung der Revision der am Installationspaket vorgenommenen Änderungen

    Standardmäßig ist die Beschreibung der Revision leer. Um der Revision eine Beschreibung hinzuzufügen, wählen Sie die gewünschte Revision aus und klicken Sie anschließend auf die Schaltfläche **Beschreibung bearbeiten**. Geben Sie im neuen Fenster einen Text zur Beschreibung der Revision ein.

Programm-Tags

Mit Kaspersky Security Center können Sie den Anwendungen in der Programm-Registry Tags hinzufügen. Ein Tag ist eine Bezeichnung, anhand derer Anwendungen gruppiert und gefunden werden können. Einer Anwendung zugewiesene Tags können als Bedingung in den Geräteauswahlen verwendet werden.

Sie können z. B. das Tag `[Browser]` erstellen und es Browsern wie Microsoft Internet Explorer, Google Chrome, Mozilla Firefox usw. zuweisen.

Programm-Tag erstellen

Um ein Anwendungs-Tag zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Tags**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Ein neues Tag-Fenster öffnet sich.
3. Geben Sie den Tag-Namen ein.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Das neue Tag wird in der Liste der Anwendungs-Tags angezeigt.

Anwendungs-Tag umbenennen

Um ein Anwendungs-Tag umzubenennen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Tags**.
2. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie umbenennen möchten, und klicken Sie auf **Bearbeiten**.

   Ein Fenster mit den Tag-Eigenschaften wird geöffnet.
3. Ändern Sie den Tag-Namen.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Das aktualisierte Tag wird in der Liste der Anwendungs-Tags angezeigt.

Einem Programm Tags zuweisen

Um einer Anwendung ein oder mehrere Tags zuzuweisen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.
2. Klicken Sie auf den Namen der Anwendung, dem Sie Tags zuweisen möchten.
3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Anwendungs-Tags an, die auf dem Administrationsserver vorhanden sind. Das Kontrollkästchen in der Spalte **Tag zugewiesen** ist für alle Tags aktiviert, die der ausgewählten Anwendung zugewiesen sind.

4. Aktivieren Sie in der Spalte **Tag zugewiesen** die Kontrollkästchen der Tags, die Sie zuweisen möchten.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Tags werden der Anwendung zugewiesen.

Zugewiesene Tags von einem Programm entfernen

Um ein oder mehrere Tags von einer Anwendung zu entfernen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.
2. Klicken Sie auf den Namen der Anwendung, von dem Sie Tags entfernen möchten.
3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Anwendungs-Tags an, die auf dem Administrationsserver vorhanden sind. Das Kontrollkästchen in der Spalte **Tag zugewiesen** ist für alle Tags aktiviert, die dem ausgewählten Programm zugewiesen sind.
4. Deaktivieren Sie in der Spalte **Tag zugewiesen** die Kontrollkästchen der Tags, die Sie entfernen möchten.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Tags werden von der Anwendung entfernt.

> Die entfernten Tags werden nicht gelöscht. Bei Bedarf können Sie diese manuell löschen.

Programm-Tag löschen

Um ein Anwendungs-Tag zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Tags**.
2. Wählen Sie in der Liste das Anwendungs-Tag aus, das Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Das Anwendungs-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Anwendungen entfernt, denen es zugewiesen war.

Überwachung und Berichterstattung

In diesem Abschnitt werden die Möglichkeiten für die Überwachung und die Berichterstellung von Kaspersky Security Center beschrieben. Diese Möglichkeiten geben Ihnen einen Überblick über Ihre Infrastruktur, die Schutzstatus und Statistiken.

Nach der Bereitstellung von Kaspersky Security Center oder während des Programmbetriebs können Sie die Funktionen für die Überwachung und für die Berichterstellung an Ihre Bedürfnisse anpassen.

Szenario: Überwachung und Berichterstattung

Dieser Abschnitt enthält ein Szenario zur Konfiguration der Funktion der Überwachung und Berichterstellung in Kaspersky Security Center.

Erforderliche Vorrausetzungen

Nach der Verteilung von Kaspersky Security Center im Unternehmensnetzwerk können Sie mit seiner Überwachung beginnen und Berichte zum Netzwerkbetrieb erstellen.

Die Überwachung und Berichterstellung in einem Unternehmensnetzwerk erfolgt in mehreren Schritten:

1. **Wechsel der Statuswerte von Geräten konfigurieren**

   Machen Sie sich mit den Einstellungen des von bestimmten Bedingungen abhängigen Gerätestatus vertraut. Wenn Sie diese Einstellungen anpassen, können Sie auch die Anzahl der Ereignisse der Ereigniskategorie *Kritisch* oder *Warnung* ändern. Beachten Sie bei der Konfiguration des Wechsels des Gerätestatus Folgendes:

   - Die neuen Einstellungen widersprechen nicht den Richtlinien zur Informationssicherheit Ihres Unternehmens.
   - Sie können rechtzeitig auf wichtige Ereignisse der Informationssicherheit in Ihrem Unternehmensnetzwerk reagieren.

2. **Einstellungen für Benachrichtigungen über Ereignisse auf Client-Geräten anpassen**

   Anleitung:

   Passen Sie die Benachrichtigungen (per E-Mail, SMS oder durch Start einer ausführbaren Datei) zu Ereignissen auf Client-Geräten an

3. **Ändern Sie die Reaktion Ihres Sicherheitsnetzwerks auf das Virenangriff-Ereignis**

   Sie können die exakten Schwellenwerte in den Eigenschaften des Administrationsservers ändern. Sie können außerdem eine strengere Richtlinie erstellen, die in einem solchen Fall aktiviert wird, oder eine Aufgabe erstellen, die bei Auftreten dieses Ereignisses ausgeführt wird.

4. **Empfohlene Aktionen für kritische und warnende Benachrichtigungen ausführen**

   Anleitung:

   Führen Sie die empfohlenen Aktionen für Ihr Unternehmensnetzwerk aus

5. **Sicherheitsstatus Ihres Unternehmensnetzwerks verfolgen**

Anleitung:

- Sehen Sie sich das Widget Schutzstatus an
- Erstellen und überprüfen Sie den Bericht über den Schutzstatus
- Erstellen und überprüfen Sie den Fehlerbericht

6. **Client-Geräte finden, die nicht geschützt sind**

   Anleitung:

   - Sehen Sie sich das Widget Neue Geräte an
   - Erstellen und überprüfen Sie den Bericht über die Bereitstellung des Schutzes

7. **Schutz der Client-Geräte überprüfen**

   Anleitung:

   - Erstellen und lesen Sie Berichte der Kategorien Schutzstatus und Bedrohungsstatistiken
   - Starten und überprüfen Sie die Ereignisauswahl mit dem Wert "Kritisch"

8. **Ereignismenge für Datenbank einschätzen und einschränken**

   Informationen über Ereignisse im Betrieb der verwalteten Anwendungen werden vom Client-Gerät übertragen und in der Administrationsserver-Datenbank registriert. Um die Belastung auf den Administrationsserver zu reduzieren, sollten Sie die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, einschätzen und einschränken.

   Anleitung:

   - Berechnung des Speicherplatzes in der Datenbank
   - Maximale Anzahl der Ereignisse einschränken

9. **Lizenzinformationen überprüfen**

   Anleitung:

   - Fügen Sie das Widget Nutzung von Lizenzschlüsseln zum Dashboard hinzu und sehen Sie es sich an
   - Erstellen und überprüfen Sie den Bericht über die Lizenzschlüsselnutzung

Ergebnisse

Nach Abschluss des Szenarios werden Sie über den Schutz Ihres Unternehmensnetzwerks informiert und können Aktionen für den weiteren Schutz des Netzwerks planen.

Über die Arten der Überwachung und Berichterstattung

Die Informationen über die Sicherheitsereignisse im Unternehmensnetzwerk werden in der Datenbank des Administrationsservers gespeichert. Basierend auf den Ereignissen bietet die Kaspersky Security Center Web Console die folgenden Arten der Überwachung und Berichterstattung in Ihrem Unternehmensnetzwerk:

- Dashboard
- Berichte
- Ereignisauswahlen
- Benachrichtigungen

Dashboard

Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen.

Berichte

Mithilfe von Berichten können Sie detaillierte, zahlenbasierte Informationen zur Sicherheit Ihres Unternehmensnetzwerkes zusammenstellen und diese Informationen in einer Datei speichern, per E-Mail versenden und ausdrucken.

Ereignisauswahlen

Die Ereignisauswahlen bieten eine Bildschirmansicht der benannten Ereignisgruppen, die aus der Administrationsserver-Datenbank ausgewählt wurden. Diese Sätze von Ereignissen sind nach den folgenden Kategorien gruppiert:

- Nach Ereigniskategorie – **Kritische Ereignisse**, **Funktionsfehler**, **Warnungen** und **Informative Ereignisse**
- Nach Zeit – **Letzte Ereignisse**
- Nach Typ – **Benutzeranfragen** und **Audit-Ereignisse**

Benutzerdefinierte Ereignisauswahlen können Sie auf der Basis von Einstellungen, die in der Oberfläche von Kaspersky Security Center Web Console verfügbar sind, erstellen und anzeigen.

Benachrichtigungen

Benachrichtigungen informieren Sie über Ereignisse und unterstützen Sie dabei, mithilfe empfohlener Maßnahmen oder mit Maßnahmen, die Sie als geeignet erachten, schneller auf diese Ereignisse zu reagieren.

Dashboard und Widgets

Dieser Abschnitt enthält Informationen über das Dashboard und die Widgets, die vom Dashboard bereitgestellt werden. Der Abschnitt enthält Anweisungen zum Verwalten von Widgets und zum Konfigurieren von Widget-Einstellungen.

Dashboard verwenden

Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen.

Das Dashboard finden Sie in der Kaspersky Security Center Web Console im Abschnitt **Überwachung und Berichterstattung** unter **Dashboard**.

Das Dashboard enthält Widgets, die angepasst werden können. Sie können aus einer großen Anzahl an unterschiedlichen Widgets auswählen, die als Kreis- oder Ringdiagramme, Tabellen, Grafiken, Balkendiagramme und Listen dargestellt werden. Die in den Widgets angezeigten Informationen werden automatisch aktualisiert und das Aktualisierungsintervall beträgt ein bis zwei Minuten. Das Aktualisierungsintervall unterscheidet sich von Widget zu Widget. Über das Einstellungsmenü können Sie die Daten eines Widgets jederzeit manuell aktualisieren.

Standardmäßig enthalten Widgets Informationen über alle Ereignisse, die in der Datenbank des Administrationsservers gespeichert sind.

Die Kaspersky Security Center Web Console besitzt eine Standardauswahl an Widgets der folgenden Kategorien:

- **Schutzstatus**
- **Bereitstellung**
- **Aktualisierungen**
- **Bedrohungsstatistiken**
- **Andere**

Einige Widgets enthalten Textinformationen und Links. Über einen Link können ausführliche Informationen angezeigt werden.

Bei der Konfiguration des Dashboards können Sie gewünschte Widgets hinzufügen, nicht benötigte Widgets ausblenden, die Größe und Darstellung der Widgets ändern, Widgets verschieben und ihre Einstellungen anpassen.

Dem Dashboard Widgets hinzufügen

So fügen Sie Widgets zum Dashboard hinzu:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Web-Widget hinzufügen oder wiederherstellen**.

3. Wählen Sie in der Liste der verfügbaren Widgets die Widgets aus, die Sie dem Dashboard hinzufügen möchten.

   Widgets sind nach Kategorien gruppiert. Um die Liste der in einer Kategorie enthaltenen Widgets anzuzeigen, klicken Sie auf das Chevron-Symbol (>) neben dem Kategorienamen.

4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Die ausgewählten Widgets werden am Ende des Dashboards hinzugefügt.

Sie können jetzt die Darstellung und Parameter der hinzugefügten Widgets bearbeiten.

Widgets im Dashboard verbergen

So verbergen Sie ein angezeigtes Widget im Dashboard:

1. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ausblenden möchten.
3. Wählen Sie **Web-Widget verbergen** aus.
4. Klicken Sie im folgenden Fenster **Warnung** auf **OK**.

Das ausgewählte Widget wird verborgen. Später können Sie dieses Widget erneut zum Dashboard hinzufügen.

Widgets auf dem Dashboard verschieben

So verschieben Sie ein Widget im Dashboard:

1. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie verschieben möchten.
3. Wählen Sie **Verschieben** aus.
4. Klicken Sie auf die Position, an die Sie das Widget verschieben möchten. Sie können nur ein anderes Widget auswählen.

Die Positionen der ausgewählten Widgets werden vertauscht.

Größe oder Darstellung von Widgets ändern

Bei Widgets, die ein Diagramm anzeigen, können Sie dessen Darstellung ändern - ein Balkendiagramm oder Liniendiagramms. Bei einigen Widgets können Sie ihre Größe ändern: kompakt, mittel oder maximal.

So ändern Sie die Widget-Darstellung:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie bearbeiten möchten.
3. Führen Sie eine der folgenden Aktionen aus:
   - Um ein Widget als Balkendiagramm anzuzeigen, wählen Sie **Diagrammtyp: Balken** aus.
   - Um ein Widget als Liniendiagramm anzuzeigen, wählen Sie **Diagrammtyp: Linien** aus.
   - Um die vom Widget eingenommene Fläche zu ändern, wählen Sie einen der Werte:
     - **Kompakt**
     - **Kompakt (nur Balken)**
     - **Mittel (Donut-Diagramm)**
     - **Mittel (Balkendiagramm)**
     - **Maximum**

Die Darstellung des ausgewählten Widgets wird geändert.

Einstellungen von Widgets ändern

Um die Einstellungen eines Widgets zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ändern möchten.
3. Wählen Sie **Einstellungen anzeigen** aus.
4. Ändern Sie im folgenden Fenster mit den Widgeteinstellungen die Widgeteinstellungen nach Bedarf.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Einstellungen des ausgewählten Widgets werden geändert.

Der Satz an Einstellungen hängt vom jeweiligen Widget ab. Nachfolgend finden Sie einige allgemeine Einstellungen:

- **Gültigkeitsbereich des Web-Widgets** (Auswahl an Objekten, für die das Widget Informationen anzeigt) – Zum Beispiel eine Administrationsgruppe oder eine Geräteauswahl.
- **Aufgabe auswählen** (Aufgabe, für die das Widget Informationen anzeigt).

- **Zeitintervall** (Zeitintervall, während dem die Informationen im Widget angezeigt werden) – Zwischen zwei angegebenen Zeitpunkten; vom angegebenen Zeitpunkt bis zum aktuellen Tag; oder vom aktuellen Tag abzüglich der angegebenen Anzahl von Tagen bis zum aktuellen Tag.

- **Werte mit Status "Kritisch"** und **Werte mit Status "Warnung"** (Regeln, welche die Farbe eines farblichen Indikators festlegen).

Nachdem Sie die Widget-Einstellungen geändert haben, können Sie die Daten im Widget manuell aktualisieren.

So aktualisieren Sie Daten in einem Widget:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.

2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie verschieben möchten.

3. Wählen Sie **Aktualisieren** aus.

   Die Daten im Widget werden aktualisiert.

Über den Nur-Dashboard-Modus

Für Mitarbeiter, die das Netzwerk nicht verwalten, aber die Statistiken zum Netzwerkschutz in Kaspersky Security Center anzeigen möchten (z. B. ein Top-Manager) können Sie den Nur-Dashboard-Modus konfigurieren. Wenn dieser Modus bei einem Benutzer aktiviert ist, wird dem Benutzer nur ein Dashboard mit einem vordefinierten Satz von Widgets angezeigt. So kann er oder sie die in den Widgets angegebenen Statistiken, wie den Schutzstatus aller verwalteten Geräte, die Anzahl der zuletzt erkannten Bedrohungen oder die Liste der häufigsten Bedrohungen im Netzwerk, überwachen.

Wenn ein Benutzer im Nur-Dashboard-Modus arbeitet, gelten die folgenden Einschränkungen:

- Das Hauptmenü wird dem Benutzer nicht angezeigt, sodass er die Schutzeinstellungen für das Netzwerk nicht ändern kann.

- Der Benutzer kann mit Widgets keine Aktionen, wie hinzufügen oder ausblenden, ausführen. Daher müssen Sie alle für den Benutzer erforderlichen Widgets auf dem Dashboard platzieren und konfigurieren, indem Sie etwa die Regel zum Zählen von Objekten oder das Zeitintervall festlegen.

Sie können sich den Nur-Dashboard-Modus nicht selbst zuweisen. Wenn Sie in diesem Modus arbeiten möchten, wenden Sie sich an einen Systemadministrator, Managed Service Provider (MSP) oder einen Benutzer mit der Berechtigung **Objekt-ACLs ändern** im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**.

Nur-Dashboard-Modus konfigurieren

Bevor Sie mit der Konfiguration des Nur-Dashboard-Modus beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie besitzen die Berechtigung **Objekt-ACLs ändern** in dem Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**. Wenn Sie diese Berechtigung nicht besitzen, fehlt der Reiter zur Konfiguration des Modus.
- Der Benutzer besitzt die Berechtigungen **Lesen** in dem Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen**.

Wenn in Ihrem Netzwerk eine Hierarchie von Administrationsservern eingerichtet ist, wechseln Sie zur Konfiguration des Nur-Dashboard-Modus auf den Server, auf dem das Benutzerkonto auf der Registerkarte **Benutzer** des Abschnitts **Benutzer und Rollen → Benutzer und Gruppen** verfügbar ist. Dabei kann es sich um einen primären oder einen physischen sekundären Server handeln. Es ist nicht möglich, den Modus auf einem virtuellen Server zu konfigurieren.

So konfigurieren Sie den Nur-Dashboard-Modus:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen → Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf den Namen des Benutzerkontos, für welches Sie das Dashboard mit Widgets anpassen möchten.
3. Öffnen Sie im folgenden Fenster mit den Kontoeinstellungen die Registerkarte **Dashboard**.

   Auf der sich öffnenden Registerkarte wird Ihnen das gleiche Dashboard angezeigt wie dem Benutzer.
4. Wenn die Option **Konsole im Nur-Dashboard-Modus anzeigen** aktiviert ist, klicken Sie auf den Umschalter, um sie zu deaktivieren.

   Wenn diese Option aktiviert ist, können auch Sie das Dashboard nicht ändern. Nachdem Sie die Option deaktiviert haben, können Sie Widgets verwalten.
5. Konfigurieren Sie das Erscheinungsbild des Dashboards. Der auf der Registerkarte **Dashboard** angezeigte Satz von Widgets steht dem Benutzer mit dem anpassbaren Konto zur Verfügung. Er oder sie kann weder die Einstellungen noch die Größe der Widgets ändern, und keine Widgets zum Dashboard hinzufügen oder daraus entfernen. Daher müssen Sie für den Benutzer die Widgets anpassen, damit er oder sie die Statistiken zum Netzwerkschutz anzeigen kann. Um dies zu tun, können Sie auf der Registerkarte **Dashboard** die gleichen Vorgänge mit den Widgets ausführen, wie im Abschnitt **Überwachung und Berichterstattung → Dashboard**:
   - Dem Dashboard neue Widgets hinzufügen.
   - Vom Nutzer nicht benötigte Widgets ausblenden.
   - Widgets verschieben, sodass sie einer bestimmten Reihenfolge entsprechen.
   - Die Größe oder das Aussehen von Widgets ändern.
   - Die Einstellungen von Widgets ändern.
6. Klicken Sie auf den Umschalter, um die Option **Konsole im Nur-Dashboard-Modus anzeigen** zu aktivieren.

Anschließend steht dem Benutzer nur noch das Dashboard zur Verfügung. Er oder sie kann Statistiken überwachen, aber die Schutzeinstellungen des Netzwerks und das Erscheinungsbild des Dashboards nicht ändern. Da für Sie das gleiche Dashboard wie für den Benutzer angezeigt wird, können auch Sie das Dashboard nicht ändern.

Wenn Sie die Option deaktiviert lassen, wird dem Benutzer das Hauptmenü angezeigt, sodass er verschiedene Aktionen in Kaspersky Security Center ausführen kann, einschließlich der Änderung von Sicherheitseinstellungen und Widgets.

7. Wenn Sie die Konfiguration des Nur-Dashboard-Modus abgeschlossen haben, klicken Sie auf **Speichern**. Erst im Anschluss wird dem Benutzer das konfigurierte Dashboard angezeigt.

8. Wenn der Benutzer zum Anzeigen der Statistiken von unterstützten Kaspersky-Anwendungen spezielle Zugriffsrechte benötigt, konfigurieren Sie diese Rechte für den Benutzer. Anschließend werden für den Benutzer die Daten der Kaspersky-Anwendungen in ihren entsprechenden Anwendungs-Widgets angezeigt.

Der Benutzer kann sich jetzt mit dem angepassten Benutzerkonto an Kaspersky Security Center anmelden und die Statistiken zum Netzwerkschutz im Nur-Dashboard-Modus überwachen.

Verwaltungs- und Schutzberichte

In diesem Abschnitt wird beschrieben, wie Sie Berichte verwenden, benutzerdefinierte Berichtsvorlagen verwalten, Berichtsvorlagen zum Generieren neuer Berichte verwenden und Aufgaben zum Berichtsversand erstellen.

Berichte verwenden

Mithilfe von Berichten können Sie detaillierte, zahlenbasierte Informationen zur Sicherheit Ihres Unternehmensnetzwerkes zusammenstellen und diese Informationen in einer Datei speichern, per E-Mail versenden und ausdrucken.

Berichte finden Sie in der Kaspersky Security Center Web Console in dem Abschnitt **Überwachung und Berichterstattung** unter **Berichte**.

Standardmäßig enthalten Berichte Informationen für die letzten 30 Tage.

Kaspersky Security Center besitzt eine Standardauswahl an Berichten der folgenden Kategorien:

- **Schutzstatus**
- **Bereitstellung**
- **Aktualisierungen**
- **Bedrohungsstatistiken**
- **Andere**

Sie können eigene Berichtsvorlagen erstellen, Berichtsvorlagen bearbeiten und löschen.

Sie können Berichte erstellen, die auf vorhandenen Vorlagen basieren, Berichte in eine Datei exportieren und Aufgaben zum Versand von Berichten erstellen.

Berichtsvorlage erstellen

Um eine Berichtsvorlage zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Berichte**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird der Assistent für das Erstellen einer Berichtsvorlage gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Geben Sie den Berichtsnamen ein und wählen Sie den Berichtstyp aus.
4. Wählen Sie im Schritt **Bereich** des Assistenten den Satz an Client-Geräten aus (Administrationsgruppe, Geräteauswahl, ausgewählte Geräte oder alle Geräte im Netzwerk), deren Daten in Berichten angezeigt werden, die auf dieser Berichtsvorlage basieren.
5. Legen Sie im Schritt **Berichtszeitraum** des Assistenten den Berichtszeitraum fest. Die folgenden Werte sind verfügbar:

   - Zwischen den beiden angegebenen Daten
   - Vom angegebenen Datum bis zum Erstellungsdatum des Berichts
   - Vom angegebenen Datum der Berichterstellung abzüglich der Tage bis zum Erstellungsdatum des Berichts

   Diese Seite wird nicht in allen Berichten angezeigt.
6. Klicken Sie auf **OK**, um den Assistenten zu schließen.
7. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Speichern und ausführen**, um die neue Berichtsvorlage zu speichern und darauf basierend einen Bericht auszuführen.

     Die Berichtsvorlage wird gespeichert. Der Bericht wird generiert.
   - Klicken Sie auf die Schaltfläche **Speichern**, um die neue Berichtsvorlage zu speichern.

     Die Berichtsvorlage wird gespeichert.

Diese neue Vorlage kann nun zum Erstellen und Anzeigen von Berichten verwendet werden.

Eigenschaften von Berichtsvorlagen anzeigen und bearbeiten

Sie können grundlegenden Eigenschaften einer Berichtsvorlage anzeigen und ändern, beispielsweise den Namen der Berichtsvorlage oder die im Bericht angezeigten Felder.

Um die Eigenschaften einer Berichtsvorlage anzuzeigen und zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Berichte**.
2. Aktivieren Sie das Kontrollkästchen neben der Berichtsvorlage, deren Eigenschaften Sie anzeigen und ändern möchten.

   Alternativ dazu können Sie zuerst den Bericht generieren und dann auf die Schaltfläche **Bearbeiten** klicken.
3. Klicken Sie auf die Schaltfläche **Eigenschaften der Berichtsvorlage öffnen**.

   Das Fenster **Bearbeiten des Berichts <Berichtsname>** wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.
4. Bearbeiten Sie die Berichtsvorlageneigenschaften:

   - Registerkarte **Allgemein**:
     - Name der Berichtsvorlage
     - **Maximale Anzahl der angezeigten Einträge**

       Wenn diese Option aktiviert ist, übersteigt die Anzahl der Einträge in der Tabelle mit detaillierten Berichtsdaten den angegebene Wert nicht.

       Die Berichtseinträge werden zuerst nach den Regeln sortiert, die im Abschnitt **Felder** → **Detail-Felder** der Eigenschaften der Berichtsvorlage angegeben sind, und nur der erste der resultierenden Einträge wird beibehalten. Die Überschrift der Tabelle mit detaillierten Berichtsdaten zeigt die angezeigte Anzahl von Einträgen und die insgesamt verfügbare Anzahl von Einträgen, die mit anderen Berichtsvorlageneinstellungen übereinstimmen.

       Wenn diese Option deaktiviert ist, zeigt die Tabelle mit detaillierten Berichtsdaten alle verfügbaren Einträge an. Es wird nicht empfohlen, diese Option zu deaktivieren. Durch die Begrenzung der Anzahl der angezeigten Berichtseinträge wird das Datenbankverwaltungssystem (DBMS) entlastet und der Zeitaufwand für das Generieren und Exportieren des Berichts verringert. Einige der Berichte enthalten zu viele Einträge. Wenn dies der Fall ist, kann es schwierig sein, sie alle zu lesen und zu analysieren. Außerdem kann es sein, dass die Erstellung eines solchen Berichts zu einer Erschöpfung der Speicherressourcen Ihres Geräts führt und Sie den Bericht dann nicht ansehen können.

       Diese Option ist standardmäßig aktiviert. Als Standardwert ist 1000 vorgegeben.
     - **Gruppe**

       Klicken Sie auf die Schaltfläche **Einstellungen**, um den Satz an Client-Geräten zu ändern, für die der Bericht erstellt wird. Bei einigen Arten von Berichten ist die Schaltfläche möglicherweise nicht verfügbar. Die aktuellen Einstellungen hängen von den Einstellungen ab, die bei der Erstellung der Berichtsvorlage angegeben wurden.
     - **Zeitintervall**

       Klicken Sie auf die Schaltfläche **Einstellungen**, um den Berichtszeitraum zu ändern. Bei einigen Arten von Berichten ist die Schaltfläche möglicherweise nicht verfügbar. Die folgenden Werte sind verfügbar:

       - Zwischen den beiden angegebenen Daten
       - Vom angegebenen Datum bis zum Erstellungsdatum des Berichts
       - Vom angegebenen Datum der Berichterstellung abzüglich der Tage bis zum Erstellungsdatum des Berichts

- **Daten von sekundären und virtuellen Administrationsservern aufnehmen**

  Wenn diese Option aktiviert ist, umfasst der Bericht die Informationen vom sekundären und vom virtuellen Administrationsserver, die dem Administrationsserver untergeordnet sind, für den die Berichtsvorlage erstellt wurde.

  Deaktivieren Sie diese Option, wenn Sie nur Daten vom aktuellen Administrationsserver anzeigen möchten.

  Diese Option ist standardmäßig aktiviert.

- **Bis Verschachtelungsebene**

  Der Bericht enthält Daten von sekundären und virtuellen Administrationsservern, die sich unter dem aktuellen Administrationsserver auf der Verschachtelungsebene befinden, die kleiner oder gleich dem angegebenen Wert ist.

  Als Standardwert ist 1 vorgegeben. Sie sollten diesen Wert ändern, wenn Sie Informationen von sekundären Administrationsservern sammeln müssen, die sich auf niedrigeren Ebenen in der Struktur befinden.

- **Intervall zum Warten auf Daten (Min.)**

  Vor Erstellen des Berichts wartet der Administrationsserver, für den die Berichtsvorlage erstellt wurde, während der angegebenen Anzahl von Minuten auf Daten von sekundären Administrationsservern. Wenn nach Ablauf dieses Zeitraums keine Daten von einem sekundären Administrationsserver eingehen, wird der Bericht dennoch ausgeführt. Anstelle der eigentlichen Daten zeigt der Bericht Daten aus dem Cache (wenn die Option **Daten von sekundären Administrationsservern im Cache zwischenspeichern** aktiviert ist) oder **N/A** (nicht verfügbar).

  Der Standardwert beträgt 5 (Minuten).

- **Daten von sekundären Administrationsservern im Cache zwischenspeichern**

  Sekundäre Administrationsserver übertragen regelmäßig Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Dort werden die übertragenen Daten im Cache gespeichert.

  Wenn der aktuelle Administrationsserver beim Erstellen des Berichts keine Daten von einem sekundären Administrationsserver empfangen kann, zeigt der Bericht Daten aus dem Cache an. Das Datum, an dem die Daten in den Cache übertragen wurden, wird ebenfalls angezeigt.

  Wenn Sie diese Option aktivieren, können Sie die Daten von sekundären Administrationsservern anzeigen, auch wenn die aktuellen Daten nicht mehr abgerufen werden können. Die angezeigten Daten können jedoch veraltet sein.

  Diese Option ist standardmäßig deaktiviert.

- **Häufigkeit des Cache-Updates (Std.)**

  Sekundäre Administrationsserver übertragen in regelmäßigen Abständen Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Sie können diesen Zeitraum in Stunden angeben. Wenn Sie 0 Stunden angeben, werden die Daten nur übertragen, wenn der Bericht generiert wird.

  Als Standardwert ist 0 vorgegeben.

- **Detaillierte Informationen von sekundären Administrationsservern übertragen**

  Im generierten Bericht enthält die Tabelle mit den detaillierten Berichtsdaten Daten von sekundären Administrationsservern des Administrationsservers, für den die Berichtsvorlage erstellt wird.

  Wenn Sie diese Option aktivieren, wird die Berichtserstellung verlangsamt und der Datenverkehr zwischen den Administrationsservern erhöht. Sie können jedoch alle Daten in einem Bericht anzeigen.

Anstatt diese Option zu aktivieren, möchten Sie möglicherweise detaillierte Berichtsdaten analysieren, um einen fehlerhaften sekundären Administrationsserver zu erkennen und dann denselben Bericht nur für den fehlerhaften Administrationsserver zu generieren.

Diese Option ist standardmäßig deaktiviert.

- Registerkarte **Felder**

  Wählen Sie die im Bericht anzuzeigenden Felder und verwenden Sie die Schaltflächen **Nach oben** und **Nach unten**, um die Reihenfolge dieser Felder zu ändern. Verwenden Sie die Schaltflächen **Hinzufügen** oder **Bearbeiten**, um festzulegen, ob die Informationen im Bericht nach den jeweiligen Feldern sortiert und gefiltert werden müssen.

  Im Abschnitt **Filter der Detail-Felder** können Sie auch auf die Schaltfläche **Filter konvertieren** klicken, um die Verwendung des erweiterten Filterformats zu starten. Mit diesem Format können Sie die in verschiedenen Feldern angegebenen Filterbedingungen mithilfe der logischen ODER-Verknüpfung kombinieren. Nach dem Klicken auf die Schaltfläche wird rechts das Bedienfeld **Filter konvertieren** geöffnet. Klicken Sie auf die Schaltfläche **Filter konvertieren**, um die Konvertierung zu bestätigen. Sie können jetzt einen konvertierten Filter mit Bedingungen aus dem Abschnitt **Detail-Felder** definieren, die mithilfe der logischen ODER-Verknüpfung angewendet werden.

  > Durch die Konvertierung eines Berichts in das Format zur Unterstützung komplexer Filterbedingungen, wird der Bericht inkompatibel zu den vorherigen Versionen von Kaspersky Security Center (11 und früher). Außerdem enthält der konvertierte Bericht keine Daten von sekundären Administrationsservern mit diesen inkompatiblen Versionen.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.
6. Schließen Sie das Fenster **Bericht <Berichtsname> bearbeiten**.

Der aktualisierte Bericht wird in der Liste der Berichtsvorlagen angezeigt.

Einen Bericht in eine Datei exportieren

Sie können einen Bericht in eine XML-, HTML- oder PDF-Datei exportieren.

So exportieren Sie einen Bericht in eine Datei:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Berichte**.
2. Aktivieren Sie das Kontrollkästchen neben dem Bericht, den Sie in eine Datei exportieren möchten.
3. Klicken Sie auf die Schaltfläche **Bericht exportieren**.
4. Ändern Sie im folgenden Fenster den Namen der Berichtsdatei im Feld **Name**. Standardmäßig stimmt der Dateiname mit dem Namen der ausgewählten Berichtsvorlage überein.
5. Wählen Sie den Berichtsdateityp aus: XML, HTML oder PDF.
6. Klicken Sie auf die Schaltfläche **Bericht exportieren**.

   Der Bericht im ausgewählten Format wird in den Standardordner Ihres Geräts heruntergeladen, oder es öffnet sich ein Standard-**Speichern unter**-Fenster in Ihrem Browser, in dem Sie die Datei an der gewünschten Stelle speichern können.

Der Bericht wird in die Datei gespeichert.

Bericht erstellen und anzeigen

Um einen Bericht zu erstellen und anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Berichte**.
2. Klicken Sie auf den Namen der Berichtsvorlage, die Sie zum Erstellen eines Berichts verwenden möchten.

   Ein Bericht, der die ausgewählte Vorlage verwendet, wird erstellt angezeigt.

Berichtsdaten werden gemäß der für den Administrationsserver eingestellten Lokalisierung angezeigt.

Im Bericht werden folgende Daten angezeigt:

- Auf der Registerkarte **Übersicht**:
  - Typ und Name des Berichts, eine Kurzbeschreibung und der Berichtszeitraum sowie Informationen darüber, für welche Gerätegruppe der Bericht erstellt wurde.
  - Graph-Diagramm mit den repräsentativsten Berichtsdaten.
  - Übersichtstabelle mit Kennziffern des Berichts.
- Auf der Registerkarte **Details** wird eine Tabelle mit detaillierten Berichtsdaten angezeigt.

Aufgabe zum Berichtsversand anlegen

Sie könne eine Aufgabe erstellen, welche die ausgewählten Berichte versendet.

Um eine Aufgabe zum Versand von Berichten zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Berichte**.
2. Aktivieren Sie die Kontrollkästchen neben den Berichtsvorlagen, für die Sie eine Aufgabe zum Versand von Berichten erstellen möchten.
3. Klicken Sie auf die Schaltfläche **Aufgabe zur Berichtzustellung erstellen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
4. Geben Sie im Schritt **Einstellungen der neue Aufgabe** des Assistenten den Namen der Aufgaben ein.

   Der Standardname lautet **Berichtsversand**. Wenn eine Aufgabe mit diesem Namen bereits existiert, wird dem Aufgabennamen eine laufende Nummer (<N>) hinzugefügt.

5. Geben Sie im Schritt **Berichtskonfiguration** des Assistenten die folgenden Einstellungen an:

   a. Berichtsvorlagen, welche die Aufgabe versenden soll.

   b. Format der Berichte: HTML, XLS oder PDF.

      Um einen Bericht ins PDF-Format zu konvertieren, wird das Tool wkhtmltopdf benötigt. Wenn Sie die Option PDF auswählen, überprüft der Administrationsserver, ob das Tool wkhtmltopdf auf dem Gerät installiert ist. Ist das Tool nicht installiert, meldet die Anwendung, dass dieses Tool auf dem Administrationsserver-Gerät installiert werden muss. Installieren Sie das Tool manuell und gehen Sie dann zum nächsten Schritt.

   c. Ob die Berichte per E-Mail gesendet werden sollen; welche Einstellungen für die Benachrichtigung per E-Mail verwendet werden sollen.

      Sie können bis zu 20 E-Mail-Adressen angeben. Mit der **Eingabetaste** können Sie E-Mail-Adressen voneinander separieren. Sie können auch eine durch Kommas getrennte Liste mit E-Mail-Adressen einfügen und anschließend die **Eingabetaste** drücken.

   d. Ob die Berichte in einem Ordner gespeichert werden sollen; ob zuvor gespeicherte Berichte in diesem Ordner überschrieben werden sollen; ob ein bestimmtes Benutzerkonto für den Zugriff auf den Ordner verwendet werden soll (bei freigegebenen Ordnern).

6. Wählen Sie im Schritt **Aufgabenzeitplan anpassen** des Assistenten den Startzeitplan für die Aufgabe aus.

   Die folgende Varianten sind für den Aufgabenzeitplan verfügbar:

   - **Manuell**

     Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

     Diese Variante ist standardmäßig ausgewählt.

   - **Alle n Minuten**

     Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

     Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

   - **Alle n Stunden**

     Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

     Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

   - **Alle n Tage**

     Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

     Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

   - **Alle n Wochen**

     Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

     Standardmäßig wird die Aufgabe jeden Montag zur aktuellen Systemzeit ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **An angegebenen Tagen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Abschluss einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filter-Symbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

7. Passen Sie in diesem Schritt des Assistenten die weiteren Einstellungen für den Aufgabenzeitplan an:

- Überprüfen oder ändern Sie im Abschnitt **Aufgabenzeitplan** den zuvor ausgewählten Zeitplan und passen Sie bei Bedarf das Zeitintervall, die Tage des Monats oder die Woche, sowie die Bedingung "Virenangriff" oder das Ausführen einer anderen Aufgabe als Auslöser für den Aufgabenstart an. Wenn ein passender Zeitplan ausgewählt ist, kann in diesem Abschnitt auch eine Startzeit angegeben werden.

- Geben Sie im Abschnitt **Zusätzliche Einstellungen** die folgenden Einstellungen an:

  - **Übersprungene Aufgaben starten**

    Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

    Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

    Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

    Diese Option ist standardmäßig deaktiviert.

  - **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

    Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

    Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

    Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  - **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

    Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

    Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

    Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

  - **Aufgabe unterbrechen, wenn deren Ausführung länger dauert als**

    Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

    Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

    Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

8. Geben Sie im Schritt **Benutzerkonto für die Ausführung der Aufgabe auswählen** des Assistenten die Anmeldeinformationen des Benutzerkontos an, unter dem die Aufgabe ausgeführt werden soll.

9. Wenn Sie nach Erstellung der Aufgabe weitere Aufgabeneinstellungen bearbeiten möchten, aktivieren Sie auf in dem Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** (diese Option ist standardmäßig aktiviert).

10. Klicken Sie auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.

    Die Aufgabe für den Versand von Berichten wird erstellt. Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet.

Berichtsvorlagen löschen

Um eine oder mehrere Berichtsvorlagen zu löschen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Berichte**.

2. Aktivieren Sie die Kontrollkästchen neben den Berichtsvorlagen, die Sie löschen möchten.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **OK**, um die Auswahl zu bestätigen.

Die ausgewählten Berichtsvorlagen werden gelöscht. Wenn diese Berichtsvorlagen in Aufgaben zum Berichtsversand verwendet wurden, werden sie auch aus den entsprechenden Aufgaben entfernt.

Ereignisse und Ereignisauswahl

Dieser Abschnitt enthält Informationen zu Ereignissen und Ereignisauswahlen, zu den in den Komponenten von Kaspersky Security Center auftretenden Ereignistypen, und zur Verwaltung der Blockierung häufiger Ereignisse.

Über Kaspersky Security Center

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Programme von Kaspersky aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert.

Ereignistypen

In Kaspersky Security Center existieren die folgenden Ereignistypen:

- Allgemeine Ereignisse. Diese Ereignisse kommen in allen verwalteten Kaspersky-Anwendungen vor. Als allgemeines Ereignis gilt beispielsweise das Ereignis Virenangriff. Allgemeine Ereignisse haben eine streng definierte Syntax und Semantik. Allgemeine Ereignisse werden beispielsweise in Berichten und auf Dashboards verwendet.

- Spezifische Ereignisse für verwaltete Kaspersky-Anwendungen. Jede verwaltete Kaspersky-Anwendung hat eine eigene Auswahl von Ereignissen.

Quellen von Ereignissen

Ereignisse können von den folgenden Programmen generiert werden:

- Komponenten von Kaspersky Security Center:
  - Administrationsserver
  - Administrationsagent
  - iOS MDM-Server
  - Exchange-Server für mobile Geräte
- Verwaltete Kaspersky-Anwendungen

  Weitere Informationen zu den Ereignissen, die von verwalteten Kaspersky-Programmen generiert werden, finden Sie in der Dokumentation des entsprechenden Programms.

Sie können die vollständige Liste der Ereignisse anzeigen, die von einer Anwendung auf der Registerkarte **Konfiguration von Ereignissen** in der Anwendungsrichtlinie generiert werden können. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen.

Ereigniskategorie von Ereignissen

Jedes Ereignis hat eine eigene Ereigniskategorie. Je nach den Bedingungen des Auftretens, können dem Ereignis verschiedene Ereigniskategorien zugewiesen werden. Es sind vier Ereigniskategorien verfügbar:

- *Kritisches Ereignis* – ein Ereignis, das auf das Auftreten eines kritischen Problems hinweist, das zu Datenverlust, einer Ausführungsstörung oder einem kritischen Fehler führen kann.

- *Funktionsfehler* – das Ereignis, das auf das Auftreten eines ernsten Problems, Fehlers oder einer Störung hinweist, welches während der Ausführung des Programms oder der Prozedur entstanden ist.

- *Warnung* – ein nicht unbedingt ernstes dem Ereignis, das jedoch auf die potentiell mögliche Entstehung eines Problems in der Zukunft hinweist. Meistens gehört die Mehrzahl der Ereignisse zu den Warnungen, wenn nach ihrem Auftreten die Ausführung der Anwendung ohne Datenverlust oder eingeschränkter Funktionalität wiederhergestellt werden kann.

- *Infomeldung* – Ereignis, das zwecks Information über das erfolgreiche Ausführen einer Operation, die korrekte Ausführung des Programms oder den Abschluss einer Prozedur auftritt.

Für jedes Ereignis ist die Speicherdauer festgelegt, die in Kaspersky Security Center angezeigt oder geändert werden kann. Einige Ereignisse werden nicht standardmäßig in der Datenbank des Administrationsservers gespeichert, da die für sie definierte Speicherdauer gleich Null ist. In externe Systeme können nur jene Ereignisse exportieren, die mindestens einen Tag in der Datenbank des Administrationsservers gespeichert werden.

Ereignisauswahlen verwenden

Die Ereignisauswahlen bieten eine Bildschirmansicht der benannten Ereignisgruppen, die aus der Administrationsserver-Datenbank ausgewählt wurden. Diese Sätze von Ereignissen sind nach den folgenden Kategorien gruppiert:

- Nach Ereigniskategorie – **Kritische Ereignisse**, **Funktionsfehler**, **Warnungen** und **Informative Ereignisse**
- Nach Zeit – **Letzte Ereignisse**
- Nach Typ – **Benutzeranfragen** und **Audit-Ereignisse**

Benutzerdefinierte Ereignisauswahlen können Sie auf der Basis von Einstellungen, die in der Oberfläche von Kaspersky Security Center Web Console verfügbar sind, erstellen und anzeigen.

Ereignisauswahlen finden Sie in Kaspersky Security Center Web Console im Abschnitt **Überwachung und Berichterstattung** unter **Ereignisauswahlen**.

Standardmäßig enthalten Ereignisauswahlen Informationen für die letzten sieben Tage.

Kaspersky Security Center besitzt eine Standardauswahl an vordefinierten Ereignisauswahlen:

- Ereignisse mit unterschiedlichen Ereigniskategorien:
  - **Kritische Ereignisse**
  - **Funktionsfehler**
  - **Warnungen**
  - **Informative Ereignisse**
- **Benutzeranfragen** (Ereignisse von verwalteten Anwendungen)
- **Letzte Ereignisse** (der letzten Woche)
- Audit-Ereignisse

Sie können auch zusätzliche benutzerdefinierte Auswahlen definieren und anpassen. In benutzerdefinierten Auswahlen können Sie Ereignisse nach den Eigenschaften der Geräte, von denen sie stammen, (Gerätenamen, IP-Bereiche und Administrationsgruppen), nach Ereignistypen und Signifikanzen, nach Anwendung und Komponentenname, sowie nach Zeitraum filtern. Es ist auch möglich, Ergebnisse der Aufgabenausführung in den Suchbereich aufzunehmen. Sie können auch ein einfaches Suchfeld verwenden, in das ein Wort oder mehrere Wörter eingegeben werden können. Alle Ereignisse, die irgendwo in den Attributen (wie Ereignisname, Beschreibung, Komponentenname) eines der eingegebenen Wörter enthalten, werden angezeigt.

Sowohl für vordefinierte als auch benutzerdefinierte Auswahlen können Sie die Zahl der angezeigten Ereignisse oder die Anzahl der Einträge, die gesucht werden sollen, begrenzen. Beide Optionen wirken sich auf die Zeit aus, die Kaspersky Security Center für die Anzeige der Ereignisse benötigt. Je größer die Datenbank ist, desto zeitaufwändiger kann der Prozess sein.

Sie können Folgendes tun:

- Eigenschaften von Ereignisauswahlen bearbeiten
- Ereignisauswahlen erstellen
- Details der Ereignisauswahlen anzeigen
- Ereignisauswahlen löschen
- Ereignisse aus der Administrationsserver-Datenbank löschen

Ereignisauswahl erstellen

Um eine Ereignisauswahl zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung → Ereignisauswahlen**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im folgenden Fenster **Neue Ereignisauswahl** die Einstellungen der neuen Ereignisauswahl an. Tun Sie dies in einem oder mehreren der Abschnitte im Fenster.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

   Das Bestätigungsfenster öffnet sich.
5. Um das Ergebnis der Ereignisauswahl anzuzeigen, lassen Sie das Kontrollkästchen **Zum Auswahlergebnis wechseln** aktiviert.
6. Klicken Sie auf **Speichern**, um die Erstellung der Ereignisauswahl zu bestätigen.

Wenn Sie das Kontrollkästchen **Zum Auswahlergebnis wechseln** aktiviert lassen, wird das Ergebnis der Ereignisauswahl angezeigt. Andernfalls wird die neue Ereignisauswahl in der Liste der Ereignisauswahl angezeigt.

Ereignisauswahl bearbeiten

Um eine Ereignisauswahl zu bearbeiten, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie bearbeiten möchten.
3. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Ein Fenster mit den Einstellungen der Ereignisauswahl wird geöffnet.
4. Bearbeiten Sie die Eigenschaften der Ereignisauswahl.

Bei vordefinierten Ereignisauswahlen können Sie nur die Eigenschaften auf den folgenden Registerkarten bearbeiten: **Allgemein** (mit Ausnahme des Namens der Auswahl), **Uhrzeit** und **Zugriffsrechte**.

Bei benutzerdefinierten Auswahlen können alle Eigenschaften bearbeitet werden.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die bearbeitete Ereignisauswahl wird in der Liste angezeigt.

Liste mit einer Ereignisauswahl anzeigen

Um eine Ereignisauswahl anzuzeigen:

1. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung → Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie starten möchten.
3. Führen Sie eine der folgenden Aktionen aus:
   - Um die Sortierung der Ergebnisse der Ereignisauswahl anzupassen, gehen Sie wie folgt vor:
     a. Klicken Sie auf die Schaltfläche **Sortierung anpassen und starten**.
     b. Geben Sie im Fenster **Sortierung der Ereignisauswahl anpassen** die Einstellungen für die Sortierung an.
     c. Klicken Sie auf den Namen der Auswahl.
   - Um die Liste der Ereignisse so anzuzeigen, wie sie auf dem Administrationsserver sortiert ist, klicken Sie auf den Namen der Auswahl.

Das Ergebnis der Ereignisauswahl wird angezeigt.

Ereignisauswahl exportieren

Mit Kaspersky Security Center können Sie eine Ereignisauswahl und deren Einstellungen in einer klo-Datei speichern. Sie können diese klo-Datei verwenden, um sowohl in Kaspersky Security Center Windows als auch in Kaspersky Security Center Linux die gespeicherte Ereignisauswahl zu importieren.

Beachten Sie, dass Sie nur benutzerdefinierte Ereignisauswahlen exportieren können. Ereignisauswahlen aus dem Standardumfang von Kaspersky Security Center (vordefinierte Auswahlen) können nicht in einer Datei gespeichert werden.

So exportieren Sie eine Ereignisauswahl:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie exportieren möchten.
   Sie können nicht mehrere Ereignisauswahlen gleichzeitig exportieren. Wenn Sie mehr als eine Auswahl auswählen, wird die Schaltfläche **Exportieren** deaktiviert.
3. Klicken Sie auf die Schaltfläche **Exportieren**.

4. Geben Sie im neuen Fenster **Speichern als** den Namen und den Pfad der Datei mit der Ereignisauswahl an und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Datei mit der Ereignisauswahl automatisch im Ordner **Downloads** gespeichert.

Ereignisauswahl importieren

Mit Kaspersky Security Center können Sie eine Ereignisauswahl aus einer klo-Datei importieren. Die klo-Datei enthält die exportierte Ereignisauswahl und deren Einstellungen.

So importieren Sie eine Ereignisauswahl:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Ereignisauswahlen**.

2. Klicken Sie auf die Schaltfläche **Importieren**, um eine Datei mit der Ereignisauswahl auszuwählen, die Sie importieren möchten.

3. Geben Sie im folgenden Fenster den Pfad zur klo-Datei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Ereignisauswahl-Datei auswählen können.

   Die Verarbeitung der Ereignisauswahl beginnt.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Ereignisauswahl erfolgreich importiert wurde, können Sie auf den Link **Importdetails anzeigen** klicken, um die Eigenschaften der Ereignisauswahl anzuzeigen.

Nach einem erfolgreichen Import wird die Ereignisauswahl in der Liste der Auswahlen angezeigt. Die Einstellungen der Ereignisauswahl werden ebenfalls importiert.

> Wenn die neu importierte Ereignisauswahl denselben Namen wie eine bereits vorhandene Ereignisauswahl besitzt, wird der Name der importierten Auswahl um den Index **(<nächste folgende Nummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Informationen zu einem Ereignis anzeigen

So zeigen Sie Informationen zu einem Ereignis an:

1. Starten Sie eine Ereignisauswahl.

2. Klicken Sie auf die Uhrzeit des gewünschten Ereignisses.

   Das Fenster **Eigenschaften des Ereignisses** wird geöffnet.

3. Im angezeigten Fenster können Sie Folgendes tun:

   - Informationen zum ausgewählten Ereignis ansehen
   - Das nächste und vorige Ereignis im Ergebnis der Ereignisauswahl öffnen

- Zum Gerät wechseln, auf dem das Ereignis eingetreten ist
- Zur Administrationsgruppe wechseln, die das Gerät enthält, auf dem das Ereignis eingetreten ist
- Zu den Aufgabeneigenschaften wechseln, wenn sich das Ereignis auf eine Aufgabe bezieht

Ereignisse in eine Datei exportieren

Mit Kaspersky Security Center können Sie Ereignisse aus einer Ereignisauswahl in einer txt-Datei speichern.

Um Ereignisse in eine Datei zu exportieren, gehen Sie wie folgt vor:

1. Starten einer Ereignisauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Ereignis.
   Sie können auch mehrere Ereignisse oder die gesamte Ereignisauswahl auswählen.
3. Klicken Sie auf die Schaltfläche **In Datei exportieren**.

Das ausgewählte Ereignis wird in eine txt-Datei exportiert.

Verlauf eines Objekts aus einem Ereignis heraus anzeigen

Sie können aus einem Ereignis zur Erstellung oder Änderung eines Objekts, das Revisionsverwaltung unterstützt, zum Revisionsverlauf dieses Objekts wechseln.

Um den Verlauf eines Objekts aus einem Ereignis heraus anzuzeigen, gehen Sie wie folgt vor:

1. Starten einer Ereignisauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Ereignis.
3. Klicken Sie auf die Schaltfläche **Revisionsverlauf**.

Der Revisionsverlauf des Objekts wird geöffnet.

Ereignisse löschen

Um eine oder mehrere Ereignisse zu löschen, gehen Sie wie folgt vor:

1. Starten einer Ereignisauswahl.
2. Aktivieren Sie die Kontrollkästchen neben den gewünschten Ereignissen.
3. Klicken Sie auf die Schaltfläche **Löschen**.

Die ausgewählten Ereignisse werden gelöscht und können nicht wiederhergestellt werden.

Ereignisauswahl löschen

Sie können nur benutzerdefinierte Ereignisauswahlen löschen. Vordefinierte Ereignisauswahlen können nicht gelöscht werden.

Um eine oder mehrere Ereignisauswahlen zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.
2. Aktivieren Sie die Kontrollkästchen neben den Ereignisauswahlen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Die Ereignisauswahl ist gelöscht.

Speicherdauer für ein Ereignis festlegen

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert. Möglicherweise sollen bestimmte Ereignisse länger oder kürzer aufbewahrt werden, als durch die Standardwerte vorgegeben. Sie können die Standardeinstellungen der Speicherdauer für ein Ereignis ändern.

Wenn Sie bestimmte Ereignisse nicht in der Administrationsserver-Datenbank speichern möchten, können Sie die entsprechende Einstellung deaktivieren. Verwenden Sie dazu die Administrationsserver-Richtlinie und die Richtlinie der Kaspersky-Anwendung oder die Administrationsserver-Eigenschaften (nur für Administrationsserver-Ereignisse). Dadurch wird die Anzahl der Ereignistypen in der Datenbank reduziert.

Je länger die Speicherdauer eines Ereignisses, desto schneller erreicht die Datenbank ihre maximale Kapazität. Eine längere Speicherdauer für ein Ereignis ermöglicht es Ihnen aber, Überwachungs- und Berichtsaufgaben über einen längeren Zeitraum durchzuführen.

So legen Sie die Speicherdauer für ein Ereignis in der Administrationsserver-Datenbank fest:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf den Namen der gewünschten Richtlinie.

   Sie können eine Richtlinie für eine verwaltete Kaspersky-Anwendung, den Administrationsagenten oder den Administrationsserver auswählen. Für den Administrationsserver können Sie außerdem die Speicherdauer der Ereignisse anpassen, indem Sie auf das Einstellungssymbol ( ) neben dem Namen des gewünschten Administrationsservers klicken.
3. Wählen Sie die Registerkarte **Konfiguration von Ereignissen** aus.

   Eine Liste der Ereignistypen, die sich auf den Abschnitt **Kritisch** beziehen, wird angezeigt. Bei Bedarf können Sie zu den Abschnitten **Funktionsfehler**, **Warnung** oder **Information** wechseln.

4. Klicken Sie in der Liste der Ereignistypen im rechten Bereich auf den Link für das Ereignis, dessen Speicherdauer Sie ändern möchten.

   Im Abschnitt **Ereignisregistrierung** des sich öffnenden Fensters ist der Umschalter **In der Administrationsserver-Datenbank speichern für (Tage)** aktiviert.

5. Geben Sie im Bearbeitungsfeld unterhalb dieser Umschalttaste die Anzahl der Tage ein, über die das Ereignis gespeichert werden soll.

6. Wenn Sie ein Ereignis nicht in der Administrationsserver-Datenbank speichern möchten, deaktivieren Sie die Option **In der Administrationsserver-Datenbank speichern für (Tage)**.

   Wenn Sie Administrationsserver-Ereignisse im Eigenschaftenfenster des Administrationsservers anpassen und wenn die Ereigniseinstellungen in der Richtlinie des Kaspersky Security Center Administrationsservers gesperrt sind, können Sie die Speicherdauer für ein Ereignis nicht ändern.

7. Klicken Sie auf **OK** und nach dem Schließen des rechten Bereichs auf die Schaltfläche **Speichern**.

   Das Eigenschaftenfenster der Richtlinie wird geschlossen.

Die Ereignisse des ausgewählten Typs, die vom Administrationsserver empfangen und gespeichert werden, besitzen ab jetzt die geänderte Speicherfrist. Für zuvor empfangene Ereignisse ändert der Administrationsserver die Speicherfrist nicht.

Ereignisse der Komponenten von Kaspersky Security Center

Jede Komponente von Kaspersky Security Center hat einen eigenen Satz von Ereignistypen. Dieser Abschnitt enthält eine Liste mit Ereignissen, die auf dem Administrationsserver von Kaspersky Security Center, im Administrationsagenten und im iOS MDM-Server auftreten können. Die Typen der Ereignisse, die in den Kaspersky-Anwendungen auftreten, sind in diesem Abschnitt nicht aufgeführt.

Für jedes Ereignis, das von einer Anwendung generiert werden kann, können Sie in der Anwendungsrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Datenstruktur der Beschreibungen von Ereignistypen

Zu jedem Ereignistyp werden der dargestellte Name, der Identifikator (ID), der alphabetische Code, die Beschreibung und die Standard-Speicherdauer angezeigt.

- **Dargestellter Name des Ereignistyps**. Dieser Text wird in Kaspersky Security Center angezeigt, wenn Sie Ereignisse konfigurieren und wenn diese auftreten.

- **Ereignistyp-ID**. Dieser numerische Code wird verwendet, wenn Sie Ereignisse zwecks Ereignisanalyse mithilfe von Drittanbieter-Tools verarbeiten.

- **Ereignistyp** (alphabetischer Code). Dieser Code wird verwendet, wenn Sie Ereignisse mithilfe der in der Datenbank von Kaspersky Security Center verfügbaren öffentlichen Ansichten durchsuchen und verarbeiten und wenn Ereignisse in ein SIEM-System exportiert werden.

- **Beschreibung**. Dieser Text beschreibt die Situationen, in denen ein Ereignis eintreffen kann, und gibt Hinweise auf weiteres Vorgehen.

- **Standard-Speicherdauer**. Das ist die Anzahl der Tage, die ein Ereignis in der Administrationsserver-Datenbank gespeichert bleibt und in der Liste der Ereignisse auf dem Administrationsserver angezeigt wird. Nach Ablauf dieses Zeitraums wird das Ereignis gelöscht. Wenn als Speicherdauer der Wert 0 angegeben ist, werden solche Ereignisse gefunden, aber nicht in der Liste der Ereignisse auf dem Administrationsserver angezeigt. Wenn Sie angegeben haben, dass solche Ereignisse im Ereignisprotokoll des Betriebssystems gespeichert werden sollen, finden Sie die Ereignisse hier.

  Sie können die Speicherdauer von Ereignissen bearbeiten:

  - Verwaltungskonsole: Speicherdauer für ein Ereignis festlegen
  - Kaspersky Security Center Web Console: Speicherdauer für ein Ereignis festlegen

Andere Daten können die folgenden Felder enthalten:

- **event_id**: eindeutige Nummer des Ereignisses in der Datenbank, automatisch generiert und zugewiesen; nicht zu verwechseln mit **Ereignistyp-ID**.
- **task_id**: ID der Aufgabe, die das Ereignis verursacht hat (falls zutreffend)
- **severity**: eine der folgenden Varianten für die Signifikanz (mit aufsteigender Signifikanz):

  0) ungültige Signifikanz

  1) Informativ

  2) Warnung

  3) Fehler

  4) Kritisch

Ereignisse des Administrationsservers

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsserver beziehen.

Ereignisse des Administrationsservers: Kritisch

Die folgende Tabelle enthält die Ereignistypen des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Kritisch**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Wenn Sie den Port in der Verwaltungskonsole im Eigenschaftenfenster des Administrationsservers angegeben haben, **veröffentlicht Kaspersky Security Center seine Metriken** und kritischen Ereignisse, damit diese im Anschluss vom Überwachungs- und Alarmsystem "Prometheus" abgerufen werden können. Prometheus ruft die Metriken und kritischen Ereignisse ab und generiert anschließend Warnungen für jedes Ereignis.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Lizenzbeschränkung wurde überschritten	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Security Center überprüft einmal täglich, ob Lizenzbeschränkungen überschritten wurden. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten die von einer Lizenz abgedeckten werden, 110% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Auch wenn dieses Ereignis eintritt, werden die Client-Geräte geschützt. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center ermittelt die Regeln zum Generieren von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.	180 Tage
Virenangriff	26 (für Schutz vor bedrohlichen Dateien)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art treten auf, wenn auf mehreren verwalteten Geräten die Anzahl an erkannten schädlichen Objekten den Schwellwert innerhalb eines kurzen Zeitraums überschreitet. Sie können auf dieses Ereignis folgendermaßen reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsservers fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird oder erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführt wird.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Virenangriff	27 (für Schutz vor E-Mail-Bedrohungen)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art treten auf, wenn auf mehreren verwalteten Geräten die Anzahl an erkannten schädlichen Objekten den Schwellwert innerhalb eines kurzen Zeitraums überschreitet. Sie können auf dieses Ereignis folgendermaßen reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsservers fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird oder erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführt wird.	180 Tage
Virenangriff	28 (für Firewall)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art treten auf, wenn auf mehreren verwalteten Geräten die Anzahl an erkannten schädlichen Objekten den Schwellwert innerhalb eines kurzen Zeitraums überschreitet. Sie können auf dieses Ereignis folgendermaßen reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsservers fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird oder erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführt wird.	180 Tage
Das Gerät wird nicht mehr verwaltet	4111	KLSRV_HOST_OUT_CONTROL	Ereignisse dieser Art treten auf, wenn ein verwaltetes Gerät ist im Netzwerk sichtbar ist, es aber über einen bestimmten Zeitraum keine Verbindung zum Administrationsserver hergestellt hat. Finden Sie heraus, warum der Administrationsagent auf diesem Gerät nicht ordnungsgemäß ausgeführt wird. Mögliche Ursachen können Netzwerkprobleme oder das Entfernen des Administrationsagenten von diesem Gerät sein.	180 Tage
Gerätestatus - "Kritisch"	4113	KLSRV_HOST_STATUS_CRITICAL	Ereignisse dieser Art treten auf, wenn einem verwalteten Gerät der Status *Kritisch* zugewiesen wird. Sie können die Bedingungen anpassen, unter denen der Gerätestatus zu *Kritisch* wechselt.	180 Tage
Die Schlüsseldatei wurde der Deny-Liste hinzugefügt	4124	KLSRV_LICENSE_BLACKLISTED	Ereignisse dieser Art treten auf, wenn Kaspersky den von Ihnen verwendeten Aktivierungscode oder die Schlüsseldatei auf die Deny-Liste setzt. Kontaktieren Sie den Technischen Support für weitere Informationen.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Eingeschränkter Funktionsmodus	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ereignisse dieser Art treten auf, wenn Kaspersky Security Center beginnt, mit Grundlegenden Funktionen und ohne Schwachstellen- und Patch-Management sowie ohne Funktionalität "Mobile Geräte verwalten", zu arbeiten. Im Folgenden die Gründe für und geeignete Reaktionen auf das Ereignis: • Die Gültigkeitsdauer der Lizenz ist abgelaufen. Um den vollen Funktionsumfang von Kaspersky Security Center zu nutzen, stellen Sie eine Lizenz bereit (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). • Der Administrationsserver verwaltet mehr Geräte, als in der Lizenz angegeben. Verschieben Sie die Geräte aus der Administrationsgruppe des Administrationsservers in die eines anderen Administrationsserver (wenn das Lizenzlimit des anderen Administrationsservers dies zulässt).	180 Tage
Die Lizenz läuft bald ab	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ereignisse dieser Art treten auf, wenn das Ablaufdatum einer kommerziellen Lizenz näher rückt. Einmal am Tag überprüft Kaspersky Security Center, ob sich das Ablaufdatum der Lizenz nähert. Veröffentlicht werden Ereignisse dieses Typs 30 Tage, 15 Tage, 5 Tage und 1 Tag vor dem Ablaufdatum der Lizenz. Die Anzahl der Tage kann nicht geändert werden. Wird der Administrationsserver an dem entsprechenden Tag vor dem Ablaufdatum der Lizenz deaktiviert, so wird das Ereignis erst am darauf folgenden Tag veröffentlicht. Wenn die kommerzielle Lizenz abläuft, stellt Kaspersky Security Center nur grundlegende Funktionen bereit. Sie können auf dieses Ereignis folgendermaßen reagieren: • Vergewissern Sie sich, dass dem Administrationsserver ein Reserve-Lizenzschlüssel hinzugefügt wurde. • Wenn Sie ein Abonnement verwenden, stellen Sie sicher, dies zu Verlängern. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag bis zum Fälligkeitsdatum an den Dienstleister überwiesen wird.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Zertifikat ist abgelaufen	4132	KLSRV_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn auf mobilen Geräten das Client-Zertifikat abläuft.	180 Tage
Das Zertifikat des Administrationsservers ist abgelaufen.	6129	ServerCertificateExpired	Ereignisse dieser Art treten auf, wenn die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ablaufen. Das abgelaufene Zertifikat muss aktualisiert werden.	180 Tage
Die Modul-Updates der Kaspersky-Anwendung wurden widerrufen	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ereignisse dieser Art treten auf, wenn nahtlose Updates von den Kaspersky-Experten zurückgerufen wurden (für diese Updates wird der Status *Zurückgerufen* angezeigt); zum Beispiel, wenn Updates auf eine neuere Version aktualisiert werden müssen. Dieses Ereignis betrifft Patches für Kaspersky Security Center. Module von Anwendungen, die durch Kaspersky verwaltet werden, sind nicht betroffen. Das Ereignis gibt den Grund an, warum das nahtlose Update nicht installiert wurde.	180 Tage
Audit: Export nach SIEM fehlgeschlagen	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Ereignisse dieser Art treten auf, wenn der Export von Ereignissen in das SIEM-System aufgrund eines Verbindungsfehlers mit dem SIEM-System fehlgeschlagen ist.	180 Tage

Ereignisse des Administrationsservers: Funktionsfehler

Die folgende Tabelle enthält die Ereignistypen des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsservers: Funktionsfehler

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Laufzeitfehler	4125	KLSRV_RUNTIME_ERROR	Ereignisse dieser Art treten bei unbekannten Problemen auf. Dabei handelt es sich meistens um DBMS-Probleme, Netzwerkprobleme und andere Hard- und Softwareprobleme. Informationen zu diesem Ereignis stehen in der Ereignisbeschreibung.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Für eine der lizenzierten Programmgruppen wurde die Beschränkung für die Anzahl von Installationen überschritten	4126	KLSRV_INVLICPROD_EXCEDED	Der Administrationsserver generiert Ereignisse dieser Art periodisch (stündlich). Ereignisse dieser Art treten auf, wenn Sie in Kaspersky Security Center die Lizenzschlüssel von Drittanbieter-Programmen verwalten und wenn die Anzahl der Installationen das Limit überschreitet, das durch den Lizenzschlüssel des Drittanbieter-Programms festgelegt ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie Drittanbieter-Anwendungen von den Geräten, auf denen sie nicht verwendet werden. • Verwenden Sie eine Drittanbieter-Lizenz für mehr Geräte. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktionen der lizenzierten Programmgruppe verwenden. Zur lizenzierten Anwendungsgruppe gehören Drittanbieter-Anwendungen, welche die von Ihnen festgelegten Kriterien erfüllen.	180 Tage
Die Abfrage des Cloud-Segments konnte nicht ausgeführt werden	4143	KLSRV_KLCLOUD_SCAN_ERROR	Ereignisse dieser Art treten auf, wenn das Abfragen eines Netzwerksegments in der Cloud-Umgebung durch den Administrationsserver fehlschlägt. Studieren Sie die Informationen in der Ereignisbeschreibung und reagieren Sie entsprechend.	Wird nicht gespeichert
Kopieren der Updates in den angegebenen Ordner nicht ausgeführt	4123	KLSRV_UPD_REPL_FAIL	Ereignisse dieser Art treten auf, wenn Programm-Updates in einen oder mehrere zusätzlich freigegebene Ordner kopiert werden. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob das Benutzerkonto, das für den Zugriff auf die Ordner verwendet wird, über Berechtigung zum Schreiben verfügt. • Prüfen Sie, ob sich der Benutzername und/oder das Kennwort zu diesen Ordnern geändert haben. • Überprüfen Sie die Internetverbindung, da sie die Ursache des Ereignisses sein kann. Folgen Sie den Anweisungen, um Datenbanken und Software-Module zu aktualisieren.	180 Tage
Kein freier Platz auf dem Datenträger	4107	KLSRV_DISK_FULL	Ereignisse dieser Art treten auf, wenn auf der Festplatte des Geräts, auf dem der Administrationsserver installiert ist, freier Speicherplatz knapp wird. Schaffen Sie freien Speicherplatz.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Kein Zugriff auf freigegebenen Ordner	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ereignisse dieser Art treten auf, wenn der Freigegebene Ordner des Administrationsservers nicht verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Überprüfen Sie, ob der Administrationsserver (auf dem sich der freigegebene Ordner befindet) angeschaltet und erreichbar ist. • Prüfen Sie, ob sich der Benutzername und/oder das Kennwort zu diesem Ordner geändert haben. • Prüfen Sie die Netzwerkverbindung.	180 Tage
Die Administrationsserver-Datenbank ist nicht verfügbar	4109	KLSRV_DATABASE_UNAVAILABLE	Ereignisse dieser Art treten auf, wenn die Administrationsserver-Datenbank nicht verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob der Remote-Server, auf dem SQL Server installiert ist, verfügbar ist. • Schauen Sie in die Protokolle des DBMS, um die Ursache für die Nichtverfügbarkeit der Administrationsserver-Datenbank zu finden. Beispielsweise kann aufgrund von präventiven Wartungsarbeiten der Remote-Server, auf dem SQL Server installiert ist, nicht verfügbar sein.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Kein freier Platz in der Administrationsserver-Datenbank	4110	KLSRV_DATABASE_FULL	Ereignisse dieser Art treten auf, wenn in der Administrationsserver-Datenbank kein freier Speicherplatz mehr vorhanden ist. Der Administrationsserver funktioniert nicht, wenn seine Datenbank die Kapazitätsgrenze erreicht hat und wenn weiteres Speichern in der Datenbank nicht möglich ist. Im Folgenden die Gründe für dieses Ereignis, in Abhängigkeit zu dem DBMS, dass Sie verwenden, sowie geeignete Reaktionen auf dieses Ereignis: • Wenn Sie als DBMS die SQL Server Express Edition verwenden: Konsultieren Sie die Dokumentation von SQL Server Express Edition und suchen Sie nach der Größenbeschränkung der von Ihnen genutzten Version. Wahrscheinlich hat die Ihre Administrationsserver-Datenbank die Größenbeschränkung der Datenbank überschritten. Begrenzung der Anzahl der Ereignisse, die in der Administrationsserver-Datenbank gespeichert werden sollen. In der Datenbank des Administrationsservers befinden sich zu viele Ereignisse, die durch die Komponente "Programmkontrolle" gesendet wurden. Sie können die Einstellungen der Richtlinie in Kaspersky Endpoint Security für Windows, die sich auf die Speicherung von Ereignissen der Programmkontrolle in der Administrationsserver-Datenbank bezieht, ändern. • Wenn Sie ein anderes DBMS als SQL Server Express Edition verwenden: Begrenzen Sie nicht die Anzahl der Ereignisse, die in der Administrationsserver-Datenbank gespeichert werden sollen. Verringern Sie die Liste an Ereignissen, die in der Administrationsserver-Datenbank gespeichert werden sollen. Überprüfen Sie die Informationen zur Auswahl des DBMS.	180 Tage

Ereignisse des Administrationsservers: Warnung

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsservers: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Ein häufiges Ereignis wurde erkannt		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Ereignisse dieser Art treten auf, wenn der Administrationsserver ein häufiges auftretendes Ereignis auf einem verwalteten Gerät erkennt. Weitere Informationen finden Sie im folgenden Abschnitt: Blockieren von häufigen auftretenden Ereignissen.	90 Tage
Lizenzbeschränkung wurde überschritten	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center überprüft einmal täglich, ob Lizenzbeschränkungen überschritten wurden. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten die von einer Lizenz abgedeckten werden, 100% bis 110% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Auch wenn dieses Ereignis eintritt, werden die Client-Geräte geschützt. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center ermittelt die Regeln zum Generieren von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Gerät war lange Zeit im Netzwerk inaktiv	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Ereignisse dieser Art treten auf, wenn ein verwaltetes Gerät für längere Zeit inaktiv erscheint. Dies ist meistens dann der Fall, wenn ein verwaltetes Gerät ausrangiert wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Löschen Sie das Gerät manuell aus der Liste der verwalteten Geräte. • Geben Sie mittels der Verwaltungskonsole oder mittels der Kaspersky Security Center Web Console den Zeitraum an, nach dem das Ereignis **Das Gerät war lange Zeit im Netzwerk inaktiv** erstellt wird. • Geben Sie mittels der Verwaltungskonsole oder mittels der Kaspersky Security Center Web Console den Zeitraum an, nach dem das Gerät automatisch aus der Gruppe entfernt wird.	90 Tage
Konflikt von Gerätenamen	4102	KLSRV_EVENT_HOSTS_CONFLICT	Ereignisse dieser Art treten auf, wenn der Administrationsserver zwei oder mehr verwaltete Geräte als ein Gerät wahrnimmt. Dies ist meistens dann der Fall, wenn ein geklontes Laufwerk für die Bereitstellung auf verwalteten Geräten verwendet wurde, und dabei der Administrationsagent auf einem Referenzgerät nicht in den dedizierten "Laufwerk klonen"-Modus versetzt wurde. Um diesen Fehler zu vermeiden, versetzen Sie den Administrationsagenten auf einem Referenzgerät in den "Laufwerk klonen"-Modus, bevor Sie das Laufwerk des Geräts klonen.	90 Tage
Gerätestatus - "Warnung"	4114	KLSRV_HOST_STATUS_WARNING	Ereignisse dieser Art treten auf, wenn einem verwalteten Gerät der Status *Warnung* zugewiesen wird. Sie können die Bedingungen anpassen, unter denen der Gerätestatus zu *Warnung* wechselt.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Für eine der lizenzierten Programmgruppen wird die Beschränkung für die Anzahl von Installationen bald überschritten	4127	KLSRV_INVLICPROD_FILLED	Ereignisse dieser Art treten auf, wenn die Anzahl der Installationen von Drittanbieter-Programmen, die in einer lizenzierten Programmgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben maximalen zulässigen Werts erreicht. Sie können auf dieses Ereignis folgendermaßen reagieren: • Wenn die Drittanbieter-Anwendung auf einigen verwalteten Geräten nicht verwendet wird, löschen Sie die Anwendung von diesen Geräten. • Wenn Sie erwarten, dass die Anzahl der Installationen der Drittanbieter-Anwendung das Maximum in nächster Zukunft übersteigt, sollten Sie im Vorfeld den Erwerb einer Drittanbieter-Lizenz für eine größere Anzahl an Geräten in Erwägung ziehen. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktionen der lizenzierten Programmgruppe verwenden.	90 Tage
Zertifikat wurde angefordert	4133	KLSRV_CERTIFICATE_REQUESTED	Ereignisse dieser Art treten auf, wenn das automatische Neuausstellen eines Zertifikats für die Funktion "Verwaltung mobiler Geräte" fehlschlägt. Im Folgenden werden die Ursachen für das Ereignis und angebrachte Reaktionen darauf ausgeführt: • Die automatische Neuausstellung wurde für ein Zertifikat initiiert, für das die Option **Zertifikat automatisch neu veröffentlichen, falls möglich** deaktiviert ist. Dies kann aufgrund eines Fehler geschehen, der bei der Erstellung des Zertifikats auftrat. Ein manuelles Neuausstellen des Zertifikats kann notwendig sein. • Wenn Sie eine Integration mit einer Public-Key-Infrastruktur verwenden, kann ein fehlendes Namensattribut des SAM-Benutzerkontos, welches für die PKI-Integration und zum Ausstellen der Zertifikate genutzt wird, die Ursache sein. Überprüfen Sie die Eigenschaften des Benutzerkontos.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Zertifikat wurde entfernt	4134	KLSRV_CERTIFICATE_REMOVED	Ereignisse dieser Art treten auf, wenn ein Administrator ein Zertifikat beliebiger Art (General, Mail, VPN) für die Funktion "Verwaltung mobiler Geräte" entfernt. Nach dem Entfernen eines Zertifikats schlägt für die mobilen Geräte, die über dieses Zertifikat verbunden sind, die Verbindung mit dem Administrationsserver fehl. Dieses Ereignis kann hilfreich sein, wenn es darum geht, Fehlfunktionen im Zusammenhang mit der Verwaltung mobiler Geräte aufzuspüren.	90 Tage
Das Zertifikat läuft ab.	6128	ServerCertificateExpiresSoon	Ereignisse dieser Art treten auf, wenn die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ablaufen. Das abgelaufene Zertifikat muss aktualisiert werden.	90 Tage
Das APNs-Zertifikat ist abgelaufen	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn ein APNs-Zertifikat abläuft. Sie müssen manuell das APNs-Zertifikat erneuern und es auf einem iOS MDM-Server installieren.	Wird nicht gespeichert
Das APNs-Zertifikat läuft bald ab	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Ereignisse dieser Art treten auf, wenn das APNs-Zertifikat in weniger als 14 Tagen abläuft. Wenn das APNs-Zertifikat abläuft, müssen Sie manuell das APNs-Zertifikat erneuern und es auf einem iOS MDM-Server installieren. Es wird empfohlen, dass Sie den Zeitpunkt für das Erneuern des APNs-Zertifikats vor das Ablaufdatum legen.	Wird nicht gespeichert
Die FCM-Nachricht konnten nicht an das mobile Gerät gesendet werden	4138	KLSRV_GCM_DEVICE_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Verwaltung mobiler Geräte" so konfiguriert ist, dass sie Firebase Cloud Messaging (FCM) für die Verbindung verwalteter Geräte mit Android Betriebssystem verwendet, und auf dem FCM-Server das Bearbeiten von empfangenen Administrationsserver-Anfragen fehlschlägt. Dies bedeutet, dass einige der verwalteten mobilen Geräte keine PUSH-Benachrichtigungen empfangen. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend. Weitere Informationen über HTTP-Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte der Dokumentation von Firebase Service (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler").	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
HTTP-Fehler beim Versenden der FCM-Nachricht an den FCM-Server	4139	KLSRV_GCM_HTTP_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Verwaltung mobiler Geräte" so konfiguriert ist, dass sie Firebase Cloud Messaging (FCM) für die Verbindung verwalteter Geräte mit Android Betriebssystem verwendet, und der FCM-Server auf eine Administrationsserver-Anfrage einen anderen HTTP-Code als 200 ("OK") zurück liefert. Im Folgenden werden die Ursachen für das Ereignis und angebrachte Reaktionen darauf ausgeführt: • Probleme mit dem FCM-Server. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend. Weitere Informationen über HTTP-Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte der Dokumentation von Firebase Service (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler"). • Probleme mit dem Proxyserver (wenn Sie einen Proxyserver benutzen). Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend.	90 Tage
Die FCM-Nachricht konnte nicht an den FCM-Server gesendet werden	4140	KLSRV_GCM_GENERAL_ERROR	Ereignisse diese Art treten auf, wenn im Rahmen der Verwendung des Firebase Cloud Messaging HTTP-Protokolls unerwartete Fehler auf dem Administrationsserver auftreten. Studieren Sie die Informationen in der Ereignisbeschreibung und reagieren Sie entsprechend. Wenn Sie selbst keine Lösung für dieses Problem ausmachen können, ist es empfehlenswert den Technischen Support von Kaspersky zu kontaktieren.	90 Tage
Auf der Festplatte ist wenig freier Platz vorhanden	4105	KLSRV_NO_SPACE_ON_VOLUMES	Ereignisse dieser Art treten auf, wenn auf dem Gerät, auf dem der Administrationsserver installiert ist, der Speicherplatz knapp wird. Schaffen Sie freien Speicherplatz.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Wenig freier Platz in der Administrationsserver-Datenbank	4106	KLSRV_NO_SPACE_IN_DATABASE	Ereignisse dieser Art treten auf, wenn der Platz in der Administrationsserver-Datenbank zu knapp ist. Wenn Sie diese Situation nicht lösen, erreicht die Administrationsserver-Datenbank bald ihre Kapazitätsgrenze und der Administrationsserver wird nicht länger funktionieren. Nachfolgend finden Sie die Ursachen für dieses Ereignis in Abhängigkeit vom DBMS, das Sie verwenden, sowie geeignete Reaktionen auf dieses Ereignis. Wenn Sie als DBMS die SQL Server Express Edition verwenden: • Konsultieren Sie die Dokumentation von SQL Server Express Edition und suchen Sie nach der Größenbeschränkung der von Ihnen genutzten Version. Wahrscheinlich wird die Datenbank Ihres Administrationsservers die Größenbeschränkung der Datenbank bald erreichen. • Begrenzung der Anzahl der Ereignisse, die in der Datenbank des Administrationsservers gespeichert werden sollen. • In der Datenbank des Administrationsservers befinden sich zu viele Ereignisse, die durch die Komponente "Programmkontrolle" gesendet wurden. Sie können die Einstellungen der Richtlinie in Kaspersky Endpoint Security für Windows, die sich auf die Speicherung von Ereignissen der Programmkontrolle in der Administrationsserver-Datenbank bezieht, ändern. Wenn Sie ein anderes DBMS als SQL Server Express Edition verwenden: • Begrenzen Sie nicht die Anzahl der Ereignisse, die in der Administrationsserver-Datenbank gespeichert werden sollen. • Reduzieren Sie die Liste an Ereignissen, die in der Administrationsserver-Datenbank gespeichert werden sollen. Überprüfen Sie die Informationen zur Auswahl des DBMS.	90 Tage
Die Verbindung mit dem sekundären Administrationsserver wurde getrennt	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum sekundären Administrationsserver unterbrochen ist. Konsultieren Sie das Kaspersky-Ereignisprotokoll des Geräts, auf dem der sekundäre Administrationsserver installiert ist, und reagieren Sie entsprechend.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Verbindung mit dem primären Administrationsserver wurde getrennt	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum primären Administrationsserver unterbrochen ist. Konsultieren Sie das Kaspersky-Ereignisprotokoll des Geräts, auf dem der primäre Administrationsserver installiert ist, und reagieren Sie entsprechend.	90 Tage
Neue Modul-Updates für Kaspersky-Anwendungen wurden registriert	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Ereignisse dieser Art treten auf, wenn der Administrationsserver für Kaspersky-Software, die auf verwalteten Geräten installiert ist, neue Updates registriert, welche eine Genehmigung für die Installation benötigen. Die Updates können Sie mithilfe der Verwaltungskonsole oder mit der Kaspersky Security Center Web Console akzeptieren oder ablehnen.	90 Tage
Die Maximalanzahl an Ereignissen in der Datenbank wurde überschritten. Es wurde mit dem Löschen von Ereignissen begonnen	4145	KLSRV_EVP_DB_TRUNCATING	Ereignisse dieser Art treten auf, wenn das Löschen älterer Ereignisse aus der Administrationsserver-Datenbank begonnen hat, nachdem die Kapazitätsgrenze der Administrationsserver-Datenbank erreicht wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Ändern Sie die maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind. • Reduzieren Sie die Liste an Ereignissen, die in der Datenbank des Administrationsservers gespeichert werden sollen.	Wird nicht gespeichert
Die Maximalanzahl an Ereignissen in der Datenbank wurde überschritten. Die Ereignisse wurden gelöscht	4146	KLSRV_EVP_DB_TRUNCATED	Ereignisse dieser Art treten auf, wenn ältere Ereignisse aus der Administrationsserver-Datenbank gelöscht wurden, nachdem die Kapazitätsgrenze der Administrationsserver-Datenbank erreicht wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Ändern Sie die zulässige maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind. • Reduzieren Sie die Liste an Ereignissen, die in der Datenbank des Administrationsservers gespeichert werden sollen.	Wird nicht gespeichert
Audit (testweise Verbindung zu SIEM-Server fehlgeschlagen)	5120	KLAUD_EV_SIEM_TEST_FAILED	Ereignisse dieser Art treten auf, wenn eine testweise Verbindung mit dem SIEM-Server fehlgeschlagen ist.	30 Tage
Das automatische Ausstellen des Zertifikats ist fehlgeschlagen		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Dieses Ereignis tritt auf, wenn beim Erstellen eines Client-Zertifikats für ein mobiles Gerät ein Fehler auftritt (ein Gerät unter einem mobilen Protokoll).	90 Tage

Ereignisse des Administrationsservers: Information

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Information**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsservers: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer	Anmerkungen
Der Lizenzschlüssel ist zu über 90% verbraucht	4097	KLSRV_EV_LICENSE_CHECK_90	30 Tage	
Neues Gerät wurde erkannt	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 Tage	
Gerät wurde automatisch zur Gruppe hinzugefügt	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 Tage	
Das Gerät wurde entsprechend einer Regel automatisch verschoben	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 Tage	
Das Gerät wurde aus der Gruppe gelöscht: Lange Zeit im Netzwerk inaktiv	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 Tage	
Die Beschränkung für die Anzahl von Installationen wird für eine der lizenzierten Programmgruppen bald überschritten (mehr als 95% verbraucht)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 Tage	
Es wurden Dateien gefunden, die zur Analyse an Kaspersky gesendet werden	4131	KLSRV_APS_FILE_APPEARED	30 Tage	
Die ID der FCM Instance hat sich auf diesem mobilen Gerät geändert	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 Tage	
Updates wurden erfolgreich in den angegebenen Ordner kopiert	4122	KLSRV_UPD_REPL_OK	30 Tage	
Die Verbindung mit dem sekundären Administrationsserver wurde hergestellt	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 Tage	
Die Verbindung mit dem primären Administrationsserver wurde hergestellt	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 Tage	
Datenbanken wurden aktualisiert	4144	KLSRV_UPD_BASES_UPDATED	30 Tage	

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer	Anmerkungen
Audit: Verbindung mit dem Administrationsserver wurde hergestellt	4147	KLAUD_EV_SERVERCONNECT	30 Tage	Ereignisse dieser Art treten auf, wenn ein Benutzer über die Verwaltungskonsole oder die Kaspersky Security Center Web Console eine Verbindung zum Administrationsserver herstellt. Diese Ereignisse enthalten Informationen über die IP-Adresse des Geräts, auf dem die MMC-basierte Verwaltungskonsole oder der Server der Kaspersky Security Center Web Console Server installiert ist.
Audit: Objekt wurde modifiziert	4148	KLAUD_EV_OBJECTMODIFY	30 Tage	Dieses Ereignis verfolgt Änderungen in den folgenden Objekten: • Administrationsgruppe • Sicherheitsgruppe • Benutzer • Paket • Aufgabe • Richtlinie • Server • Virtueller Server
Audit: Objektstatus wurde geändert	4150	KLAUD_EV_TASK_STATE_CHANGED	30 Tage	Dieses Ereignis tritt beispielsweise auf, wenn eine Aufgabe mit einem Fehler beendet wurde.
Audit: Gruppeneinstellungen wurden modifiziert	4149	KLAUD_EV_ADMGROUP_CHANGED	30 Tage	
Audit: Die Verbindung mit dem Administrationsserver wurde unterbrochen	4151	KLAUD_EV_SERVERDISCONNECT	30 Tage	
Audit: Objekteigenschaften wurden geändert	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 Tage	Dieses Ereignis verfolgt Änderungen der folgenden Eigenschaften: • Benutzer • Lizenz • Server • Virtueller Server
Audit: Benutzerberechtigungen wurden geändert	4153	KLAUD_EV_OBJECTACLMODIFIED	30 Tage	
Audit: Die Chiffrierschlüssel wurden vom Administrationsserver importiert oder exportiert	5100	KLAUD_EV_DPEKEYSEXPORT	30 Tage	
Audit: (testweise Verbindung zu SIEM-Server erfolgreich)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 Tage	Dieses Ereignis tritt auf, wenn eine testweise Verbindung mit dem SIEM-Server erfolgreich war.

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer	Anmerkungen
Reservezertifikat wurde erstellt		ServerReserveCertificateCreated	30 Tage	Dieses Ereignis tritt auf, wenn das Zertifikat des Administrationsservers erstellt wurde.
Zertifikat wird erneuert		ServerCertificateRenewed	30 Tage	Dieses Ereignis tritt auf, wenn das Zertifikat des Administrationsservers erneuert wurde.

Die Ereignisse **Reservezertifikat wurde erstellt** und **Zertifikat wird erneuert** werden nur dann automatisch vom Administrationsserver veröffentlicht und in der Verwaltungskonsole angezeigt, wenn die Vorgänge, die diesen Ereignissen entsprechen, für die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ausgeführt werden.

Ereignisse des Administrationsagenten

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsagenten beziehen.

Ereignisse des Administrationsagenten: Funktionsfehler

Die folgende Tabelle enthält die Ereignistypen des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsagenten: Funktionsfehler

Angezeigter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Fehler bei der Update-Installation	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn das automatische Update und Patchen von Komponenten von Kaspersky Security Center fehlgeschlagen sind. Das Ereignis betrifft nicht die Updates von verwalteten Kaspersky-Anwendungen. Lesen Sie die Ereignisbeschreibung. Ein möglicher Grund für dieses Ereignis ist ein Windows-Problem auf dem Administrationsserver. Wenn die Beschreibung ein Problem in der Windows-Konfiguration erwähnt, beheben Sie dieses Problem.	30 Tage
Installation des Updates für Drittherstellersoftware fehlgeschlagen	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion Schwachstellen- und Patch-Management sowie die Funktion Verwaltung mobiler Geräte verwendet werden, und wenn das Update einer Drittanbieter-Software nicht erfolgreich war. Überprüfen Sie, ob der Link zur Software für Drittanbieter gültig ist. Lesen Sie die Ereignisbeschreibung.	30 Tage

Angezeigter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Installation der Updates von Windows-Update fehlgeschlagen	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn Windows Updates nicht erfolgreich waren. Windows-Updates in der Richtlinie des Administrationsagenten anpassen. Lesen Sie die Ereignisbeschreibung. Suchen Sie in der Microsoft Knowledge Base nach dem Fehler. Wenden Sie sich an den technischen Support von Microsoft, wenn Sie das Problem nicht selbst lösen können.	30 Tage
Benutzerverwaltung: Fehler	7723	KLNAG_EV_USR_MNG_ERR	Ereignis bei einer allgemeinen Warnung.	30 Tage
Das Zurücksetzen der sudoers-Datei auf den Referenzwert ist fehlgeschlagen	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der beim Ersetzen der sudoers-Datei aufgetreten ist.	30 Tage
Die Installation der Root-Zertifikate ist fehlgeschlagen	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der bei der Installation von Zertifikaten aufgetreten ist.	30 Tage
Die Root-Zertifikate konnten nicht gelöscht werden	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der beim Entfernen von Zertifikaten aufgetreten ist.	30 Tage

Ereignisse des Administrationsagenten: Warnung

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsagenten: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Während der Installation des Updates des Software-Moduls wurde eine Warnung zurückgegeben	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 Tage
Installation des Updates für die Drittherstellersoftware wurde mit einer Warnung abgeschlossen	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 Tage
Installation des Updates für Drittherstellersoftware wurde aufgeschoben	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 Tage
Es ist ein Sicherheitsproblem aufgetreten	549	GNRL_EV_APP_INCIDENT_OCCURED	30 Tage
KSN-Proxy wurde gestartet. Überprüfen der KSN-Verfügbarkeit nicht ausgeführt	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 Tage
Benutzerverwaltung: Warnungen	7722	KLNAG_EV_USR_MNG_WRN	30 Tage
Die gefundene sudoers-Datei entspricht nicht dem Referenzwert	7724	KLNAG_EV_SUDOER_DIFFERENT	30 Tage

Ereignisse des Administrationsagenten: Information

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Information**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsagenten: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Update für Software-Module wurde erfolgreich installiert	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 Tage
Installation des Updates des Software-Moduls wurde gestartet	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 Tage
Programm wurde installiert	7703	KLNAG_EV_INV_APP_INSTALLED	30 Tage
Programm wurde deinstalliert	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 Tage
Überwachtes Programm wurde installiert	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 Tage
Überwachtes Programm wurde deinstalliert	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 Tage
Drittherstellerprogramm wurde installiert	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 Tage
Neues Gerät wurde hinzugefügt	7708	KLNAG_EV_DEVICE_ARRIVAL	30 Tage
Gerät wurde entfernt	7709	KLNAG_EV_DEVICE_REMOVE	30 Tage
Neues Gerät wurde erkannt	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 Tage
Gerät wurde autorisiert	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 Tage
Windows Desktopfreigabe: Datei wurde gelesen	7712	KLUSRLOG_EV_FILE_READ	30 Tage
Windows Desktopfreigabe: Datei wurde geändert	7713	KLUSRLOG_EV_FILE_MODIFIED	30 Tage
Windows Desktopfreigabe: Das Programm wurde gestartet	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 Tage
Windows Desktopfreigabe: Gestartet	7715	KLUSRLOG_EV_WDS_BEGIN	30 Tage
Windows Desktopfreigabe: Beendet	7716	KLUSRLOG_EV_WDS_END	30 Tage
Update für Drittherstellersoftware wurde erfolgreich installiert	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 Tage
Installation des Updates von Drittherstellersoftware wurde gestartet	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 Tage
KSN-Proxy wurde gestartet. Überprüfung der KSN-Verfügbarkeit wurde erfolgreich abgeschlossen	7719	KSNPROXY_STARTED_CON_CHK_OK	30 Tage
KSN Proxy wurde angehalten	7720	KSNPROXY_STOPPED	30 Tage

Ereignisse des iOS MDM-Servers

Dieser Abschnitt informiert über die Ereignisse, die sich auf den iOS MDM-Server beziehen.

Ereignisse des iOS MDM-Servers: Funktionsfehler

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center iOS MDM-Servers mit der Signifikanz **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des iOS MDM-Servers: Funktionsfehler

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Die Profilliste konnte nicht angefordert werden	PROFILELIST_COMMAND_FAILED	30 Tage
Das Profil konnte nicht installiert werden	INSTALLPROFILE_COMMAND_FAILED	30 Tage
Das Profil konnte nicht entfernt werden	REMOVEPROFILE_COMMAND_FAILED	30 Tage
Die Liste der Provisioning-Profile konnte nicht angefordert werden	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 Tage
Das Provisioning-Profil konnte nicht installiert werden	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 Tage
Das Provisioning-Profil konnte nicht entfernt werden	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 Tage
Die Liste der digitalen Zertifikate konnte nicht angefordert werden	CERTIFICATELIST_COMMAND_FAILED	30 Tage
Die Liste der installierten Programme konnte nicht angefordert werden	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 Tage
Allgemeine Informationen zum mobilen Gerät konnten nicht angefordert werden	DEVICEINFORMATION_COMMAND_FAILED	30 Tage
Sicherheitsinformationen konnten nicht angefordert werden	SECURITYINFO_COMMAND_FAILED	30 Tage
Das mobile Gerät konnte nicht gesperrt werden	DEVICELOCK_COMMAND_FAILED	30 Tage
Das Kennwort konnte nicht gelöscht werden	CLEARPASSCODE_COMMAND_FAILED	30 Tage
Die Daten des mobilen Geräts konnten nicht gelöscht werden	ERASEDEVICE_COMMAND_FAILED	30 Tage
Die App konnte nicht installiert werden	INSTALLAPPLICATION_COMMAND_FAILED	30 Tage
Der Gutscheincode für die App konnte nicht installiert werden	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 Tage
Die Liste der verwalteten Apps konnte nicht angefordert werden	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 Tage
Die verwaltete App konnte nicht entfernt werden	REMOVEAPPLICATION_COMMAND_FAILED	30 Tage
Die Roaming-Einstellungen wurden abgelehnt	SETROAMINGSETTINGS_COMMAND_FAILED	30 Tage
Bei der Ausführung der App ist ein Fehler aufgetreten	PRODUCT_FAILURE	30 Tage
Das Ergebnis der Befehlsausführung enthält ungültige Daten	MALFORMED_COMMAND	30 Tage
Die Benachrichtigung (Push Notification) konnte nicht gesendet werden	SEND_PUSH_NOTIFICATION_FAILED	30 Tage
Der Befehl konnte nicht gesendet werden	SEND_COMMAND_FAILED	30 Tage
Das Gerät wurde nicht gefunden	DEVICE_NOT_FOUND	30 Tage

Ereignisse des iOS MDM-Servers: Warnung

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center iOS MDM-Servers mit der Signifikanz **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des iOS MDM-Servers: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Es wurde versucht, das gesperrte mobile Gerät anzuschließen	INACTICE_DEVICE_TRY_CONNECTED	30 Tage
Profil wurde entfernt	MDM_PROFILE_WAS_REMOVED	30 Tage
Versuch einer wiederholten Verwendung des Client-Zertifikats	CLIENT_CERT_ALREADY_IN_USE	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Inaktives Gerät wurde gefunden	FOUND_INACTIVE_DEVICE	30 Tage
Ein Gutscheincode ist erforderlich	NEED_REDEMPTION_CODE	30 Tage
Profil gehört zu einer Richtlinie, die vom Gerät gelöscht wurde	UMDM_PROFILE_WAS_REMOVED	30 Tage

Ereignisse des iOS MDM-Servers: Information

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center iOS MDM-Servers mit der Signifikanz **Information**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des iOS MDM-Servers: Information

Dargestellter Name des Ereignistyps	Ereignistyp	Standard-Speicherdauer
Das neue mobile Gerät wurde angeschlossen	NEW_DEVICE_CONNECTED	30 Tage
Profilliste wurde erfolgreich angefordert	PROFILELIST_COMMAND_SUCCESSFULL	30 Tage
Das Profil wurde erfolgreich installiert	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 Tage
Das Profil wurde erfolgreich gelöscht	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 Tage
Die Liste der Provisioning-Profile wurde erfolgreich angefordert	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 Tage
Das Provisioning-Profil wurde erfolgreich installiert	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 Tage
Das Provisioning-Profil wurde erfolgreich gelöscht	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 Tage
Liste der digitalen Zertifikate wurde erfolgreich angefordert	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 Tage
Die Liste der installierten Programme wurde erfolgreich angefordert	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 Tage
Allgemeine Informationen zum mobilen Gerät wurden erfolgreich angefordert	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 Tage
Sicherheitsinformationen wurden erfolgreich angefordert	SECURITYINFO_COMMAND_SUCCESSFULL	30 Tage
Das mobile Gerät wurde erfolgreich gesperrt	DEVICELOCK_COMMAND_SUCCESSFULL	30 Tage
Das Kennwort wurde erfolgreich gelöscht	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 Tage
Die Daten auf dem mobilen Gerät wurden erfolgreich bereinigt	ERASEDEVICE_COMMAND_SUCCESSFULL	30 Tage
App wurde erfolgreich installiert	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 Tage
Gutscheincode für die App wurde erfolgreich installiert	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 Tage
Die Liste der verwalteten Apps wurde erfolgreich angefordert	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 Tage
Die verwaltete App wurde erfolgreich entfernt	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 Tage
Roaming-Einstellungen wurden erfolgreich übernommen	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 Tage

Häufige auftretende Ereignisse blockieren

Dieser Abschnitt enthält Informationen zur Verwaltung des Blockierens häufig auftretender Ereignisse sowie zum Aufheben der Blockade häufig auftretender Ereignisse.

Über das Blockieren von häufig auftretenden Ereignissen

Ein verwaltetes Programm (z. B. Kaspersky Endpoint Security für Windows), das auf einem oder mehreren verwalteten Geräten installiert ist, sendet möglicherweise viele Ereignisse des gleichen Typs an den Administrationsserver. Das Empfangen häufig auftretender Ereignisse kann die Administrationsserver-Datenbank überlasten und führt zum Überschreiben anderer Ereignisse. Der Administrationsserver beginnt, die am häufigsten auftretenden Ereignisse zu blockieren, wenn die Anzahl aller empfangenen Ereignisse den für die Datenbank festgelegten Grenzwert überschreitet.

Der Administrationsserver blockiert den Empfang von häufig auftretenden Ereignissen automatisch. Sie können die häufig auftretenden Ereignisse nicht selbst blockieren und auch nicht festlegen, welche Ereignisse blockiert werden sollen.

Um herauszufinden, ob ein Ereignis blockiert wird, können Sie die Liste mit Benachrichtigung anzeigen oder überprüfen, ob das Ereignis im Abschnitt **Blockieren häufiger Ereignisse** des Administrationsservers aufgeführt ist. Wenn das Ereignis blockiert ist, können Sie Folgendes tun:

- Wenn Sie verhindern möchten, dass die Datenbank überschrieben wird, können Sie das Empfangen dieser Ereignistypen weiterhin blockieren.
- Wenn Sie beispielsweise den Grund für das häufige Senden eines Ereignisses an den Administrationsserver ermitteln möchten, können Sie häufig auftretende Ereignisse entsperren und die Ereignisse dieses Typs auf diese Weise weiterhin empfangen.
- Wenn Sie die häufig auftretenden Ereignisse weiterhin so lange empfangen möchten, bis sie wieder blockiert werden, können Sie für die häufig auftretenden Ereignisse die Blockierung entfernen.

Das Blockieren häufig auftretender Ereignissen verwalten

Der Administrationsserver blockiert den automatischen Empfang von häufig auftretenden Ereignissen, aber Sie können die Blockade aufheben und häufig auftretende Ereignisse weiterhin empfangen. Sie können außerdem den Empfang häufig auftretender Ereignisse blockieren, deren Blockade Sie zuvor aufgehoben haben.

So verwalten Sie das Blockieren von häufig auftretenden Ereignissen:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Blockieren häufiger Ereignisse** aus.

3. In dem Abschnitt **Blockieren häufiger Ereignisse**:

   - Wenn Sie das Blockieren des Empfangs häufig auftretender Ereignisse aufheben möchten:

     a. Wählen Sie die häufig auftretenden Ereignisse aus, die Sie entsperren möchten, und klicken Sie anschließend auf die Schaltfläche **Ausschließen**.

     b. Klicken Sie auf die Schaltfläche **Speichern**.

   - Um häufig auftretende Ereignisse zu blockieren:

     a. Wählen Sie die häufig auftretenden Ereignisse aus, die Sie blockieren möchten, und klicken Sie auf **Blockieren**.

     b. Klicken Sie auf die Schaltfläche **Speichern**.

Der Administrationsserver empfängt die entsperrten häufig auftretenden Ereignisse und empfängt keine blockierten häufig auftretende Ereignisse.

Die Blockade häufig auftretender Ereignisse aufheben

Sie können die Blockade für häufig auftretende Ereignisse aufheben und diese so lange empfangen, bis der Administrationsserver diese häufig auftretenden Ereignissen erneut blockiert.

So heben Sie die Blockade für häufig auftretende Ereignisse auf:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ().

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Blockieren häufiger Ereignisse** aus.

3. Wählen Sie im Abschnitt **Blockieren häufiger Ereignisse** die Arten häufig auftretender Ereignisse, für die Sie die Blockade aufheben möchten.

4. Klicken Sie auf **Blockade aufheben**.

Das häufig auftretende Ereignis wird aus der Liste der häufig auftretenden Ereignisse entfernt. Der Administrationsserver empfängt Ereignisse dieses Typs.

Benachrichtigungen und Gerätestatus

Dieser Abschnitt enthält Informationen zum Anzeigen von Benachrichtigungen, zum Konfigurieren der Zustellung von Benachrichtigungen, zum Verwenden des Gerätestatus und zum Aktivieren der Änderung von Statuswerten der Geräte.

Benachrichtigungen verwenden

Benachrichtigungen informieren Sie über Ereignisse und unterstützen Sie dabei, mithilfe empfohlener Maßnahmen oder mit Maßnahmen, die Sie als geeignet erachten, schneller auf diese Ereignisse zu reagieren.

Je nach ausgewählter Benachrichtigungsmethode, stehen die folgenden Benachrichtigungstypen zur Verfügung:

- Bildschirmbenachrichtigungen
- Benachrichtigungen per SMS
- Benachrichtigungen per E-Mail
- Benachrichtigungen per ausführbarer Datei oder Skript

Bildschirmbenachrichtigungen

Bildschirmbenachrichtigungen informieren Sie über Ereignisse, die in Ereigniskategorien gruppiert sind (*Kritisch*, *Warnung*, und *Information*).

Bildschirmbenachrichtigungen können zwei Status haben:

- *Geprüft*. Dies bedeutet, dass Sie die für diese Nachricht empfohlenen Maßnahmen durchgeführt haben oder dass Sie der Nachricht diesen Status manuell zugewiesen haben.
- *Ungeprüft*. Dies bedeutet, dass Sie die für diese Nachricht empfohlenen Maßnahmen nicht durchgeführt haben oder dass Sie der Nachricht diesen Status nicht manuell zugewiesen haben.

Standardmäßig enthält die Liste mit Benachrichtigungen die Nachrichten mit dem Status *Ungeprüft*.

Sie können Ihr Unternehmensnetzwerk durch das Anzeigen der Bildschirmbenachrichtigungen kontrollieren und in Echtzeit auf diese reagieren.

Benachrichtigungen per E-Mail, SMS und ausführbarer Datei oder Skript

Kaspersky Security Center bietet die Möglichkeit, Ihr Unternehmensnetzwerk zu kontrollieren, indem Nachrichten über alle Ereignisse, die Sie als wichtig einstufen, versandt werden. Für jedes Ereignis können Sie Benachrichtigungen per E-Mail, per SMS oder durch das Starten einer ausführbaren Datei oder eines Skripts konfigurieren.

Nach dem Erhalten von Benachrichtigungen per E-Mail oder SMS können Sie entscheiden, wie Sie auf das Ereignis reagieren. Die Reaktion sollte diejenige sein, die für Ihr Unternehmensnetzwerk am geeignetsten ist. Durch den Start einer ausführbaren Datei oder eines Skripts, geben Sie eine vordefinierte Reaktion auf ein Ereignis an. Sie können den Start einer ausführbaren Datei oder eines Skripts auch als erste Reaktion auf ein Ereignis in Erwägung ziehen. Nachdem die ausführbare Datei gestartet wurde, können Sie weitere Schritte unternehmen, um auf das Ereignis zu reagieren.

Bildschirmbenachrichtigungen anzeigen

Es gibt drei Möglichkeiten, um Benachrichtigungen auf dem Bildschirm anzuzeigen:

- In dem Abschnitt **Überwachung und Berichterstattung** → **Benachrichtigungen**. Hier können Sie Nachrichten über vordefinierte Kategorien anzeigen.
- In einem separaten Fenster, welches unabhängig davon, in welchem Abschnitt Sie sich gerade befinden, geöffnet werden kann. In diesem Fall können Sie Nachrichten als geprüft markieren.
- In dem Widget **Benachrichtigungen nach ausgewählter Signifikanz** im Abschnitt **Überwachung und Berichterstattung** → **Dashboard**. In dem Widget können Sie nur Nachrichten der Ereigniskategorien *Kritisch* und *Warnung* ansehen.

Sie können Aktionen ausführen, z. B. als Reaktion auf ein Ereignis.

Um Benachrichtigungen vordefinierter Kategorien anzuzeigen:

1. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Benachrichtigungen**.

   Im linken Bereich ist die Kategorie **Alle Benachrichtigungen** ausgewählt, und im rechten Bereich werden alle Benachrichtigungen angezeigt.

2. Wählen Sie im linken Bereich eine der drei Kategorien:

   - **Bereitstellung**
   - **Geräte**
   - **Schutz**
   - **Updates** (Diese Kategorie umfasst Benachrichtigungen über Kaspersky-Anwendungen, die zum Download verfügbar sind und Benachrichtigungen über Updates der Antiviren-Datenbanken, die heruntergeladen wurden.)
   - **Exploit-Prävention**
   - **Administrationsserver** (Diese Kategorie umfasst Ereignisse, die nur den Administrationsserver betreffen.)
   - **Nützliche Links** (Diese Kategorie umfasst Links zu Ressourcen von Kaspersky, z. B. zum Technischen Support von Kaspersky, dem Forum von Kaspersky, der Seite für Lizenzverlängerung und der Kaspersky IT Enzyklopädie.)

   Eine Liste mit Nachrichten zu den ausgewählten Kategorien wird angezeigt. Die Liste enthält Folgendes:

- Symbol, das dem Thema der Benachrichtigung entspricht: Bereitstellung (), Schutz (), Update (), Geräteverwaltung (), Exploit-Prävention (), Administrationsserver ().
- Ereigniskategorie der Nachricht. Angezeigt werden Nachrichten mit den folgenden Ereigniskategorien: **Kritische Benachrichtigungen** (), **Warnende Benachrichtigungen** (), **Informative Benachrichtigungen**. Die Benachrichtigungen in der Liste sind nach Ereigniskategorien gruppiert.
- **Benachrichtigung**. Dies beinhaltet eine Beschreibung der Nachricht.

- **Aktion**. Dies beinhaltet einen Link zu einer empfohlenen Sofortmaßnahme. Sie können beispielsweise durch klicken des Links in die Datenverwaltung wechseln und Sicherheitsanwendungen auf Geräten installieren, oder sich eine Liste mit Geräten oder Ereignissen anzeigen lassen. Nachdem die empfohlene Maßnahme für die Nachricht durchgeführt wurde, wird der Nachricht der Status *Geprüft* zugewiesen.

- **Status registriert**. Dies beinhaltet die Anzahl der vergangenen Tage und Stunden, seit die Nachricht auf dem Administrationsserver registriert wurde.

Um Bildschirmbenachrichtigungen nach Ereigniskategorien in einem separaten Fenster anzuzeigen:

1. Klicken Sie in der rechten oberen Ecke der Kaspersky Security Center Web Console auf das Flaggen-Symbol ( ).

   Wenn das Flaggen-Symbol einen roten Punkt besitzt, existieren Nachrichten, die noch nicht gelesen wurden.

   Es öffnet sich ein Fenster mit der Liste von Nachrichten. Standardmäßig ist die Registerkarte **Alle Benachrichtigungen** ausgewählt und die Nachrichten sind nach Ereigniskategorie gruppiert: *Kritisch*, *Warnung*, und *Information*.

2. Wählen Sie die Registerkarte **System** aus.

   Die Liste der Nachrichten mit den Ereigniskategorien *Kritisch* ( ) und *Warnung* ( ) wird angezeigt. Die Liste der Nachrichten enthält Folgendes:

   - Eine Farbmarkierung. Kritische Benachrichtigungen sind rot markiert. Warnende Benachrichtigungen sind gelb markiert.
   - Symbol, welches das Thema der Benachrichtigung angibt: Bereitstellung ( ), Schutz ( ), Update ( ), Geräteverwaltung ( ), Exploit-Prävention ( ), Administrationsserver ( ).
   - Eine Beschreibung der Nachricht.
   - Flaggen-Symbol. Das Flaggen-Symbol ist grau, wenn Benachrichtigungen der Status *Nicht gelesen* zugewiesen wurden. Wenn Sie das graue Flaggen-Symbol auswählen und einer Nachricht den Status *Gelesen* zuweisen, ändert sich die Farbe des Symbols zu weiß.
   - Link zur empfohlenen Maßnahme. Wenn Sie auf den Link klicken und anschließend die empfohlene Maßnahme durchführen, erhält die Nachricht den Status *Geprüft*.
   - Die Anzahl der vergangenen Tage seit die Nachricht auf dem Administrationsserver registriert wurde.

3. Wählen Sie die Registerkarte **Mehr** aus.

   Die Liste der Benachrichtigungen mit der Ereigniskategorie *Information* wird angezeigt.

   Der Aufbau der Liste ist identisch mit dem der Liste für die Registerkarte **System** (siehe oben). Der einzige Unterschied ist die fehlende Farbmarkierung.

Sie können Benachrichtigungen nach dem Datumsintervall, in welchem sie auf dem Administrationsserver registriert wurden, filtern. Benutzen Sie das Kontrollkästchen **Filter anzeigen** um den Filter zu verwalten.

Um Bildschirmbenachrichtigungen im Widget anzuzeigen:

1. Wählen Sie im Abschnitt **Dashboard** den Punkt **Web-Widget hinzufügen oder wiederherstellen**.

2. Klicken Sie in dem sich öffnenden Fenster auf die Kategorie **Andere**, wählen Sie das Widget **Benachrichtigungen nach ausgewählter Signifikanz** aus, und klicken Sie auf Hinzufügen.

   Das Widget erscheint jetzt auf der Registerkarte **Dashboard**. Standardmäßig zeigt das Widget Benachrichtigungen mit der Ereigniskategorie *Kritisch* an.

   Sie können in dem Widget auf die Schaltfläche **Einstellungen** klicken und die Einstellungen des Widgets ändern, um Nachrichten mit der Ereigniskategorie *Warnung* anzuzeigen. Oder Sie können mittels **Benachrichtigungen nach ausgewählter Signifikanz**, ein weiteres Widget mit der Ereigniskategorie *Warnung* hinzufügen.

   Die Liste der Benachrichtigungen ist im Widget in seiner Größe eingeschränkt und enthält zwei Nachrichten. Diese zwei Nachrichten entsprechen den zwei neuesten Ereignissen.

Im Widget enthält die Liste der Nachrichten Folgendes:

- Symbol, das dem Thema der Benachrichtigung entspricht: Bereitstellung (), Schutz (), Update (), Geräteverwaltung (), Exploit-Prävention (), Administrationsserver ().
- Eine Beschreibung der Nachricht mit einem Link zur empfohlenen Maßnahme. Wenn Sie auf den Link klicken und anschließend eine empfohlene Maßnahme durchführen, erhält die Nachricht den Status *Geprüft*.
- Die Anzahl der vergangenen Tage oder Stunden seit die Nachricht auf dem Administrationsserver registriert wurde.
- Ein Link zu weiteren Benachrichtigungen. Durch das Anklicken des Links gelangen Sie in den Unterabschnitt **Benachrichtigungen** des Abschnitts **Überwachung und Berichterstattung**.

Über die Varianten für den Gerätestatus

Kaspersky Security Center weist jedem verwalteten Gerät einen Status zu. Der jeweilige Status hängt davon ab, ob die vom Benutzer definierten Bedingungen erfüllt sind. Wenn Kaspersky Security Center einem Gerät einen Status zuweist, wird in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). Beispiel: Wenn einem verwalteten Gerät der Status *Kritisch* zugewiesen wurde, da die Bedingung *Die Datenbanken sind veraltet* erfüllt ist und für das Gerät später das Sichtbarkeits-Flag gesetzt wurde, erhält das Gerät den Status *OK*. Wenn Kaspersky Security Center ein Gerät innerhalb von zwei Stunden nicht im Netzwerk findet, wird das Sichtbarkeits-Flag des Gerätes auf *Nicht sichtbar* gesetzt.

Es gibt folgende Statusvarianten:

- *Kritisch* oder *Kritisch / Sichtbar*
- *Warnung* oder *Warnung / Sichtbar*
- *OK* oder *OK / Sichtbar*

Die folgende Tabelle enthält die erforderlichen Standardbedingungen, nach denen einem Gerät der Status *Kritisch* oder *Warnung* zugewiesen wird, sowie alle möglichen Werte.

Bedingungen für das Zuweisen der Status an das Gerät

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Es wurde keine Sicherheitsanwendung installiert	Auf dem Gerät ist der Administrationsagent installiert, aber es wurde keine Sicherheitsanwendung installiert.	• Umschalter aktiviert. • Umschalter deaktiviert.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Zu viele Viren gefunden	Auf dem Gerät wurden als Ergebnis der Ausführung einer Aufgabe zur Virensuche (beispielsweise der Aufgabe zur *Schadsoftware-Untersuchung*) mehrere Viren gefunden, und die Anzahl der gefundenen Viren übersteigt den angegebenen Wert.	Über 0.
Die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die der Administrator festgelegt hat	Das Gerät ist im Netzwerk sichtbar, aber die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die vom Administrator (in der Bedingung) für den Gerätestatus eingestellt wurde.	• Beendet. • Angehalten. • Wird ausgeführt.
Die letzte Schadsoftware-Untersuchung liegt lange zurück	Das Gerät ist im Netzwerk sichtbar und es wurde eine Sicherheitsanwendung auf dem Gerät installiert, aber es wurde weder die Aufgabe zur *Schadsoftware-Untersuchung*, noch die Aufgabe zur lokalen Untersuchung innerhalb des angegebenen Zeitintervalls ausgeführt. Die Bedingung gilt nur für Geräte, die vor mehr als sieben Tagen zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.
Die Datenbanken sind veraltet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung wurde auf dem Gerät installiert, aber die Antiviren-Datenbanken wurden auf diesem Gerät nicht innerhalb des angegebenen Zeitintervalls aktualisiert. Die Bedingung gilt nur für Geräte, die vor mehr als einem Tag zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.
Die letzte Verbindung liegt lange zurück	Der Administrationsagent ist auf dem Gerät installiert, es wurde allerdings nicht innerhalb des angegebenen Zeitintervalls mit dem Administrationsserver verbunden, da es deaktiviert ist.	Über 1 Tag.
Aktive Bedrohungen werden erkannt	Die Anzahl der unbearbeiteten Objekte im Ordner **Aktive Bedrohungen** übersteigt den angegebenen Wert.	Über 0 Elemente.
Neustart erforderlich	Das Gerät ist im Netzwerk sichtbar, aber eine Anwendung erfordert aufgrund einer der angegeben Bedingungen einen Neustart des Gerätes, der nicht innerhalb des festgelegten Zeitraums ausgeführt wurde.	Über 0 Minuten.
Es sind inkompatible Anwendungen installiert	Das Gerät ist im Netzwerk sichtbar, aber infolge der Inventarisierung der Software durch den Administrationsagenten wurden auf dem Gerät inkompatible Anwendungen gefunden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden Schwachstellen in Programmen erkannt	Das Gerät ist im Netzwerk sichtbar und der Administrationsagent ist auf dem Gerät installiert, aber die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* hat in den Programmen auf dem Gerät Schwachstellen mit der angegebenen Signifikanz gefunden.	• Kritisch. • Hoch. • Normal. • Ignorieren, wenn die Schwachstelle nicht geschlossen werden kann. • Ignorieren, wenn das Update für die Installation bestimmt wurde.
Lizenz abgelaufen	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz ist abgelaufen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Die Lizenz läuft bald ab	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz auf dem Gerät läuft in weniger als der angegebenen Anzahl an Tagen ab.	Weniger als 0 Tage.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Die letzte Suche nach Windows-Updates liegt lange zurück	Das Gerät ist im Netzwerk sichtbar, aber die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* wurde nicht innerhalb des angegebenen Zeitintervalls ausgeführt.	Über 1 Tag.
Ungültiger Verschlüsselungsstatus	Der Administrationsagent ist auf dem Gerät installiert, aber das Ergebnis der Verschlüsselung des Geräts entspricht dem angegebenen Wert.	• Entspricht nicht der Richtlinie aufgrund der Ablehnung durch den Benutzer (nur für externe Geräte). • Entspricht nicht der Richtlinie wegen eines Fehlers. • Bei der Übernahme der Richtlinie – Neustart erforderlich. • Es wurde keine Verschlüsselungsrichtlinie festgelegt. • Nicht unterstützt. • Bei der Übernahme der Richtlinie.
Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie	Die Einstellungen des mobilen Geräts unterscheiden sich von den in der Richtlinie von Kaspersky Endpoint Security für Android festgelegten Einstellungen beim Ausführen der Untersuchung der Übereinstimmungsregeln.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden unbearbeitete Sicherheitsprobleme erkannt	Auf dem Gerät sind unbearbeitete Sicherheitsvorfälle vorhanden. Sicherheitsvorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten verwalteten Kaspersky-Anwendungen als auch manuell durch den Administrator erstellt werden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Gerätestatus wird vom Programm bestimmt	Der Gerätestatus wird von der verwalteten Anwendung bestimmt. Verwaltete Geräte können einen Status besitzen, der von den verwalteten Anwendungen unabhängig von den Einstellungen von Kaspersky Security Center bestimmt wird. Wenn der Status zu einem der Werte zurückkehrt, die durch Kaspersky Security Center bestimmt werden, weist der Administrationsserver einem verwalteten Gerät den kritischsten Status zu, der von der verwalteten Anwendung zurückgegeben und vom Administrationsserver zugewiesen wurde. Statuswerte, die von verwalteten Anwendungen bestimmt werden, besitzen Beschreibungen, die ebenfalls von den verwalteten Anwendungen stammen. Sie können diese Beschreibungen in der Liste der verwalteten Geräte in der Spalte **Statusbeschreibung**.	• Umschalter ist deaktiviert. • Umschalter ist aktiviert.
Kein Platz auf dem Datenträger des Geräts	Der freie Speicherplatz auf dem Datenträger ist kleiner als der angegebene Wert oder das Gerät konnte nicht mit dem Administrationsserver synchronisiert werden. Der Status *Kritisch* oder *Warnung* wird in den Status *OK* geändert, wenn das Gerät erfolgreich mit dem Administrationsserver synchronisiert wird und der freie Speicherplatz auf dem Gerät dem angegebenen Wert entspricht oder diesen überschreitet.	Über 0 MB.
Das Gerät wird nicht mehr verwaltet	Bei der Gerätesuche ist das Gerät im Netzwerk sichtbar, aber es sind mehr als drei Synchronisierungsversuche mit dem Administrationsserver fehlgeschlagen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Der Schutz ist deaktiviert	Das Gerät ist im Netzwerk sichtbar, aber die Sicherheitsanwendung auf dem Gerät ist länger deaktiviert, als im Zeitintervall angegeben. In diesem Fall lautet der Status der Sicherheitsanwendung *Angehalten* oder *Fehler* und unterscheidet sich von den folgenden Statuswerten *Wird gestartet*, *Wird ausgeführt* oder *Wird angehalten*.	Über 0 Minuten.
Die Sicherheitsanwendung wurde nicht gestartet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung ist auf dem Gerät installiert, wurde aber nicht gestartet.	• Umschalter deaktiviert. • Umschalter aktiviert.

Kaspersky Security Center ermöglicht eine Konfiguration der automatischen Umschaltung des Status von Geräten in der Administrationsgruppe bei Erfüllung der angegebenen Bedingungen. Bei Erfüllung der festgelegten Bedingungen wird dem Client-Gerät einer der folgenden Statuswerte verliehen: *Kritisch* oder *Warnung*. Sind die festgelegten Bedingungen nicht erfüllt, so erhält das Client-Gerät den Status *OK*.

Verschiedenen Werten einer einzelnen Bedingung können verschiedene Statusvarianten entsprechen. Beispiele: Wenn die Bedingung **Die Datenbanken sind veraltet** den Wert **Über 3 Tage** besitzt, erhält das Client-Gerät standardmäßig den Status *Warnung*; für den Wert **Über 7 Tage** wird der Status *Kritisch* zugewiesen.

Wenn Sie Kaspersky Security Center von der vorhergehenden Version aktualisieren, ändern sich nicht die Werte zum Zuweisen des Status *Kritisch* oder *Warnung* für die Bedingung **Die Datenbanken sind veraltet**.

Wechsel der Statuswerte von Geräten konfigurieren

Sie können die Bedingungen ändern, um einem Gerät den Status *Kritisch* oder *Warnung* zuzuweisen.

Um die Änderungen des Gerätestatus auf Kritisch zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Kritisch** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Kritisch" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Kritisch*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.
9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Warnung** aus.

5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Warnung" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Warnung*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.

9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Einstellungen für das Versenden von Benachrichtigungen anpassen

Sie können die Benachrichtigung über Ereignisse im Kaspersky Security Center konfigurieren. Je nach ausgewählter Benachrichtigungsmethode, stehen die folgenden Benachrichtigungstypen zur Verfügung:

- E-Mail: Beim Auftreten eines Ereignisses sendet Kaspersky Security Center Benachrichtigungen an die angegebenen E-Mail-Adressen.
- SMS: Beim Auftreten eines Ereignisses sendet Kaspersky Security Center Benachrichtigungen an die angegebenen Telefonnummern.
- Ausführbare Datei: Wählen Sie die ausführbare Datei, die auf dem Administrationsserver gestartet wird, wenn ein Ereignis eintritt.

So können Sie die Benachrichtigung über Ereignisse in Kaspersky Security Center konfigurieren:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Klicken Sie auf den Abschnitt **Benachrichtigung**, und wählen Sie im rechten Bereich die Registerkarte für die gewünschte Benachrichtigungsmethode:

   - **E-Mail**

     Auf der Registerkarte **E-Mail** können Sie die Ereignisprotokollierung per E-Mail konfigurieren.

     Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen.

Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- Windows-Netzwerkname (NetBIOS-Name) des Geräts
- DNS-Name des SMTP-Servers

Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig wird Portnummer 25 verwendet.

Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren, können Sie mehrere MX-Einträge von IP-Adressen für denselben DNS-Namen des SMTP-Servers verwenden. Der gleiche DNS-Name kann mehrere MX-Einträge mit unterschiedlichen Prioritäten für das Empfangen von E-Mail-Nachrichten enthalten. Der Administrationsserver versucht, entsprechend der Priorität der MX-Einträge, die E-Mail-Nachrichten in aufsteigender Reihenfolge an den SMTP-Server zu senden.

Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren und die Verwendung von TLS-Einstellungen deaktivieren, ist es empfehlenswert, die DNSSEC-Einstellungen auf Ihrem Servergerät als zusätzliche Schutzmaßnahme beim Senden von E-Mail-Nachrichten zu verwenden.

Wenn Sie die Option **ESMTP-Authentifizierung verwenden** aktivieren, können Sie die ESMTP-Authentifizierungseinstellungen in den Feldern **Benutzername** und **Kennwort** angeben. Standardmäßig ist die Option deaktiviert und die ESMTP-Authentifizierungseinstellungen sind nicht verfügbar.

Sie können die TLS-Einstellungen einer Verbindung mit einem SMTP-Server angeben:

- **TLS nicht verwenden**

Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

- **TLS verwenden, wenn dies vom SMTP-Server unterstützt wird**

Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

- **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen**

Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen** ausgewählt haben, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können Zertifikate für eine TLS-Verbindung angeben, indem Sie auf den Link **Zertifikate angeben** klicken:

- Geben Sie eine Datei mit SMTP-Server-Zertifikat an:

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center prüft, ob das Zertifikat eines SMTP-Servers auch von eine vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

- Geben Sie die Datei des Client-Zertifikats an:

Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen Zertifizierungsstelle. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

- X-509-Zertifikat:

Sie müssen eine Datei mit dem Zertifikat und eine Datei mit dem privaten Schlüssel angeben. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Laden der Dateien ist spielt keine Rolle. Wenn beide Dateien geladen sind, müssen Sie das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- pkcs12-Container:

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

Geben Sie im Feld **Betreff** den Betreff der E-Mail an. Sie können dieses Feld leer lassen.

Wählen Sie in der Dropdown-Liste **Betreffsvorlage** die Vorlage für Ihren Betreff aus. Eine durch die ausgewählte Vorlage bestimmte Variable wird automatisch in das Feld **Betreff** eingefügt. Sie können einen E-Mail-Betreff erstellen, indem Sie mehrere Betreffsvorlagen auswählen.

Geben Sie im Feld **E-Mail-Adresse des Absenders** die E-Mail-Adresse des Absenders an. Wenn Sie dieses Feld leer lassen, wird standardmäßig die Empfängeradresse verwendet. Wir raten davon ab, fingierte E-Mail-Adressen zu verwenden.

Das Feld **Benachrichtigungstext** enthält Standard-Text mit der Information zum Ereignis, der beim Eintreten des Ereignisses versendet wird. Dieser Text enthält Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne. Sie können den Text der Meldung bearbeiten und weitere Platzhalter mit relevanten Informationen zum Ereignis hinzufügen.

> Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Wenn Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, die das Programm innerhalb des angegebenen Zeitintervalls versenden darf.

Wenn Sie auf die Schaltfläche **Testnachricht senden** klicken, können Sie prüfen, ob die Benachrichtigungen korrekt angepasst sind: Das Programm sendet eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen.

- **SMS**

Auf der Registerkarte **SMS** können Sie den Versand von SMS-Benachrichtigungen zu verschiedenen Ereignissen an ein Mobiltelefon anpassen. SMS-Nachrichten werden über ein Mail-Gateway gesendet.

Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- Windows-Netzwerkname (NetBIOS-Name) des Geräts
- DNS-Name des SMTP-Servers

Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig wird Portnummer 25 verwendet.

Wenn die Option **ESMTP-Authentifizierung verwenden** aktiviert ist, können Sie die ESMTP-Authentifizierungseinstellungen in den Feldern **Benutzername** und **Kennwort** angeben. Standardmäßig ist die Option deaktiviert und die ESMTP-Authentifizierungseinstellungen sind nicht verfügbar.

Sie können die TLS-Einstellungen einer Verbindung mit einem SMTP-Server angeben:

- **TLS nicht verwenden**

Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

- **TLS verwenden, wenn dies vom SMTP-Server unterstützt wird**

Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

- **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen**

Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen** ausgewählt haben, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können die Zertifikatsdatei des SMTP-Servers angeben, indem Sie auf den Link **Zertifikate angeben** klicken:

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center prüft, ob das Zertifikat eines SMTP-Servers auch von eine vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen. Die Benachrichtigungen werden an die Telefonnummern gesendet, die den angegebenen E-Mail-Adressen zugewiesen sind.

Geben Sie im Feld **Betreff** den Betreff der E-Mail an.

Wählen Sie in der Dropdown-Liste **Betreffsvorlage** die Vorlage für Ihren Betreff aus. Eine Variable entsprechend der ausgewählten Vorlage wird in das Feld **Betreff** eingefügt. Sie können einen E-Mail-Betreff erstellen, indem Sie mehrere Betreffsvorlagen auswählen.

Geben Sie im Feld **E-Mail-Adresse des Absenders: Wenn diese Einstellung nicht angegeben ist, wird stattdessen die Empfängeradresse verwendet. Achtung: Es wird nicht empfohlen, eine fiktive E-Mail-Adresse zu verwenden** die E-Mail-Adresse des Absenders an. Wenn Sie dieses Feld leer lassen, wird standardmäßig die Empfängeradresse verwendet. Wir raten davon ab, fingierte E-Mail-Adressen zu verwenden.

Geben Sie im Feld **Telefonnummern der SMS-Nachrichtenempfänger** die Mobiltelefonnummern der Empfänger der SMS-Benachrichtigungen ein.

Geben Sie im Feld **Benachrichtigungstext** den Text mit der Information zum Ereignis ein, der beim Eintreten des Ereignisses versendet wird. Dieser Text kann Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne enthalten.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Klicken Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren**, um die maximale Anzahl an Benachrichtigungen anzugeben, die das Programm während des angegebenen Zeitintervalls versenden darf.

Klicken Sie auf **Testnachricht senden**, um zu prüfen, ob Sie die Benachrichtigungen korrekt konfiguriert haben: Das Programm sendet dann eine Testnachricht an die von Ihnen angegebenen Empfänger.

- **Start einer ausführbaren Datei**

  Wenn diese Methode der Zustellung von Benachrichtigungen ausgewählt ist, können Sie im Eingabefeld die Anwendung angeben, die gestartet wird, sobald ein Ereignis eintritt.

  Geben Sie im Feld **Ausführbare Datei, die auf dem Administrationsserver gestartet wird, wenn ein Ereignis eintritt** den Ordner und den Namen der auszuführenden Datei an. Bevor Sie die Datei angeben, bereiten Sie die diese vor und geben Sie die Platzhalter an die für die Ereignisdetails stehen, die in der Nachricht gesendet werden sollen. Der von Ihnen angegebene Ordner und die Datei müssen sich auf dem Administrationsserver befinden.

  Wenn Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, die das Programm innerhalb des angegebenen Zeitintervalls versenden darf.

3. Definieren Sie auf der Registerkarte die Benachrichtigungseinstellungen.

4. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Administrationsservers zu schließen.

Die gespeicherten Einstellungen für die Zustellung von Benachrichtigungen werden auf alle Ereignisse angewendet, die in Kaspersky Security Center auftreten.

Für die Einstellungen des Administrationsservers, einer Richtlinie oder des Programms können Sie im Abschnitt **Konfiguration von Ereignissen** die Benachrichtigungseinstellungen für bestimmte Ereignisse überschreiben.

Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei

Kaspersky Security Center bietet die Möglichkeit, den Administrator durch den Start einer ausführbaren Datei über Ereignisse auf den Client-Geräten zu benachrichtigen. Diese ausführbare Datei muss eine weitere ausführbare Datei mit Parameterplatzhaltern für das Ereignis enthalten, die dem Administrator übermittelt werden müssen (siehe Abbildung unten).

Parameterplatzhalter zur Beschreibung des Ereignisses

Parameterplatzhalter	Beschreibung des Parameterplatzhalters
%SEVERITY%	Signifikanz des Ereignisses. Mögliche Werte: • **Information** • **Warnung** • **Fehler** • **Kritisch**
%COMPUTER%	Name des Geräts, auf dem das Ereignis eingetreten ist. Die maximale Länge des Gerätenamens beträgt 256 Zeichen.
%DOMAIN%	Domänenname des Geräts, auf dem das Ereignis eingetreten ist.
%EVENT%	Name des Ereignistyps. Die maximale Länge des Namens des Ereignistyps beträgt 50 Zeichen.
%DESCR%	Ereignisbeschreibung. Die maximale Länge der Beschreibung beträgt 1000 Zeichen.
%RISE_TIME%	Zeitpunkt der Ereigniserstellung.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Aufgabenname. Die maximale Länge des Aufgabennamens beträgt 100 Zeichen.
%KL_PRODUCT%	Name der Anwendung.
%KL_VERSION%	Versionsnummer der Anwendung.
%KLCSAK_EVENT_SEVERITY_NUM%	Signifikanzkennzahl des Ereignisses. Mögliche Werte: • 1 – **Information** • 2 – **Warnung** • 3 – **Fehler** • 4 – **Kritisch**
%HOST_IP%	IP-Adresse des Geräts, auf dem das Ereignis eingetreten ist.
%HOST_CONN_IP%	IP-Adresse der Verbindung auf dem Geräts, auf dem das Ereignis eingetreten ist.

Beispiel:
Ausführbare Datei zur Benachrichtigung über Ereignisse (z. B. script1.bat), innerhalb der eine weitere ausführbare Datei (z. B. script2.bat) mit dem Parameterplatzhalter %COMPUTER% gestartet wird. Beim Auftreten eines Ereignisses auf dem Gerät des Administrators wird die Datei script1.bat gestartet, die wiederum die Datei script2.bat mit dem Parameter %COMPUTER% startet. Dadurch erhält der Administrator den Namen des Geräts, auf dem das Ereignis aufgetreten ist.

Kaspersky-Mitteilungen

In diesem Abschnitt wird beschrieben, wie Sie Kaspersky-Mitteilungen verwenden, konfigurieren und deaktivieren.

Über Kaspersky-Mitteilungen

Im Abschnitt mit den Kaspersky-Mitteilungen (**Überwachung und Berichterstattung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center und den verwalteten Programmen, die auf den verwalteten Geräten installiert sind. Kaspersky Security Center aktualisiert die Informationen in diesem Abschnitt regelmäßig: Veraltete Mitteilungen werden entfernt und neue Informationen hinzugefügt.

Kaspersky Security Center zeigt nur die Kaspersky-Mitteilungen an, die sich auf den derzeit verbundenen Administrationsserver und die auf dessen verwalteten Geräten installierten Kaspersky-Anwendungen beziehen. Die Mitteilungen werden für jeden Typ von Administrationsserver individuell angezeigt – primär, sekundär oder virtuell.

Der Administrationsserver benötigt eine Internetverbindung, um Kaspersky-Mitteilungen zu empfangen.

Die Mitteilungen enthalten Informationen der folgenden Typen:

- Sicherheitsrelevante Mitteilungen

  Mit sicherheitsrelevanten Mitteilungen werden die in Ihrem Netzwerk installierten Kaspersky-Anwendungen auf dem neuesten Stand und voll funktionsfähig gehalten. Die Mitteilungen können Informationen über kritische Updates für Kaspersky-Anwendungen, Korrekturen für gefundene Schwachstellen und Methoden zum Beheben sonstiger Probleme in Kaspersky-Anwendungen enthalten. Sicherheitsrelevante Mitteilungen sind standardmäßig aktiviert. Wenn Sie keine Mitteilungen erhalten möchten, können Sie diese Funktion deaktivieren.

  Um Ihnen die Informationen anzuzeigen, die Ihrer Netzwerkschutzkonfiguration entsprechen, sendet Kaspersky Security Center Daten an die Kaspersky-Cloud-Server und empfängt nur die Mitteilungen, welche die in Ihrem Netzwerk installierten Kaspersky-Anwendungen betreffen. Der Datensatz, der an die Server gesendet werden kann, ist im Endbenutzer-Lizenzvertrag beschrieben, den Sie bei der Installation des Kaspersky Security Center Administrationsservers akzeptieren.

- Marketing-Mitteilungen

  Marketing-Mitteilungen enthalten Informationen über Sonderangebote für Ihre Kaspersky-Anwendungen, Werbung und Neuigkeiten von Kaspersky. Marketing-Mitteilungen sind standardmäßig deaktiviert. Diese Art von Mitteilungen erhalten Sie nur, wenn Sie Kaspersky Security Network (KSN) aktiviert haben. Sie können Marketing-Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

  Um Ihnen nur relevante Informationen anzuzeigen, die für den Schutz Ihrer Netzwerkgeräte und für Ihren Aufgabenbereich hilfreich sein können, sendet Kaspersky Security Center Daten an die Kaspersky-Cloud-Server und empfängt die entsprechenden Mitteilungen. Der Datensatz, der an die Server gesendet werden kann, wird im Abschnitt "Verarbeitete Daten" der KSN-Erklärung beschrieben.

Neue Informationen werden in Abhängigkeit ihrer Wichtigkeit in zwei Kategorien eingeteilt:

1. Kritische Information
2. Wichtige Neuigkeiten
3. Warnung
4. Information

Wenn im Abschnitt "Mitteilungen von Kaspersky" neue Informationen erscheinen, zeigt Kaspersky Security Center Web Console ein Benachrichtigungssymbol, welches der Ereigniskategorie der Mitteilungen entspricht. Sie können auf das Symbol klicken, um sich die Mitteilung im Abschnitt "Mitteilungen von Kaspersky" anzusehen.

Sie können die Einstellungen für Kaspersky-Mitteilungen konfigurieren, die Mitteilungskategorien wählen, die Sie ansehen möchten, und festlegen, wo das Benachrichtigungssymbol angezeigt werden soll.

Einstellungen für die Kaspersky-Mitteilungen festlegen

Im Abschnitt Mitteilungen von Kaspersky können Sie die Einstellungen für Kaspersky-Mitteilungen konfigurieren, die Mitteilungskategorien wählen, die Sie ansehen möchten, und festlegen, wo das Benachrichtigungssymbol angezeigt werden soll.

So konfigurieren Sie die Mitteilungen von Kaspersky:

1. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung → Mitteilungen von Kaspersky**.
2. Klicken Sie auf den Link **Einstellungen**.

   Das Fenster mit den Einstellungen für die Kaspersky-Mitteilungen wird geöffnet.
3. Geben Sie die folgenden Einstellungen an:

   - Wählen Sie die Ereigniskategorie der Mitteilungen, die Sie ansehen möchten. Die Mitteilungen anderer Kategorien werden nicht angezeigt.
   - Geben Sie an, wo das Benachrichtigungssymbol angezeigt werden soll. Das Symbol kann in allen Abschnitt der Konsole, sowie im Abschnitt **Überwachung und Berichterstattung** und in dessen Unterabschnitten angezeigt werden.
4. Klicken Sie auf die Schaltfläche **OK**.

   Die Einstellungen der Kaspersky-Mitteilungen sind angegeben.

Kaspersky-Mitteilungen deaktivieren

Im Abschnitt Mitteilungen von Kaspersky (**Überwachung und Berichterstattung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center und den verwalteten Programmen, die auf den verwalteten Geräten installiert sind. Wenn Sie keine Mitteilungen von Kaspersky erhalten möchten, können Sie diese Funktion deaktivieren.

Die Kaspersky-Mitteilungen enthalten zwei Arten von Informationen: sicherheitsrelevante Mitteilungen und Marketing-Mitteilungen. Sie können jeden Mitteilungstyp getrennt deaktivieren.

Um sicherheitsrelevante Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Mitteilungen von Kaspersky** aus.
3. Stellen Sie den Umschalter auf die Position **Sicherheitsrelevante Mitteilungen Deaktiviert**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

   Jetzt sind die Kaspersky-Mitteilungen deaktiviert.

Marketing-Mitteilungen sind standardmäßig deaktiviert. Marketing-Mitteilungen erhalten Sie nur, wenn Sie Kaspersky Security Network (KSN) aktiviert haben. Sie können diese Art von Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

Um Marketing-Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.
3. Deaktivieren Sie die Option **Kaspersky Security Network verwenden Aktiviert**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

   Jetzt sind die Marketing-Mitteilungen deaktiviert.

Informationen über die Erkennung von Bedrohungen anzeigen

Sie können die Anzeige von Informationen über Alarme aktivieren oder deaktivieren.

*So aktivieren oder deaktivieren Sie die Anzeige von Abschnitt **Alarme** im Hauptmenü:*

1. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Einstellungen der Benutzeroberfläche.**
2. Aktivieren oder deaktivieren Sie im folgenden Fenster **Einstellungen der Benutzeroberfläche** die Option **Alarme von EDR anzeigen**.
3. Klicken Sie auf **Speichern**.

Die Konsole zeigt den Unterabschnitt **Alarme** im Abschnitt **Überwachung und Berichterstattung** des Hauptmenüs an. Im Unterabschnitt **Alarme** können Sie Informationen über die Erkennung von Bedrohungen auf den Endpunktgeräten anzeigen. Wenn Sie einen Lizenzschlüssel für EDR Optimum hinzufügen, zeigt Kaspersky Security Center Web Console automatisch den Unterabschnitt **Alarme** im Abschnitt **Überwachung und Berichterstattung** des Hauptmenüs an. Sie können auch ein Widget hinzufügen, welches Informationen zu Warnungen anzeigt.

> Der Unterabschnitt **Alarme** wird nur dann automatisch angezeigt, wenn Sie vor dem Aktivieren der Option **Alarme von EDR anzeigen** den Lizenzschlüssel für EDR Optimum hinzugefügt haben. Wenn Sie den Lizenzschlüssel erst nach dem Aktivieren der Option **Alarme von EDR anzeigen** hinzugefügt haben, wird der Unterabschnitt **Alarme** erst angezeigt, nachdem Sie die Option erneut aktiviert haben.

Damit detaillierte Informationen über erkannte Bedrohungen korrekt auf der Alarm-Karte angezeigt werden, müssen Sie das Plug-in für Kaspersky Endpoint Agent und die kompatible Version des Plug-ins für Kaspersky Endpoint Security installieren (Kaspersky Endpoint Security für Linux 12.1 oder höher, Kaspersky Endpoint Security for Mac 12.1 oder höher, oder Kaspersky Endpoint Security für Windows 12.6 oder höher).

Verwenden Sie das Menü **Filter**, um Benachrichtigungen nach Datum und Feldwerten zu filtern.

Das Feld **Objekttyp** enthält die folgenden Werte:

- Unbekannt
- Phishing-Link
- Virus
- Trojaner
- Schädliches Programm

- Backdoor
- Wurm
- Anderes Programm
- Adware
- Pornware
- Gefährliches gepacktes Programm
- Gefährliches Verhalten

Das Feld **Automatische Antwort** enthält die folgenden Werte:

- Schädliches Objekt erkannt
- Objekt gelöscht
- Objekt desinfiziert
- Objekt konnte nicht desinfiziert werden
- Objekt in Quarantäne verschoben
- Kennwortgeschütztes Archiv gefunden
- Virus gefunden

Cloud Discovery

Kaspersky Security Center ermöglicht es Ihnen, die Verwendung von Cloud-Diensten auf verwalteten Windows-Geräten zu überwachen und den Zugriff auf unerwünschte Cloud-Dienste zu blockieren. Cloud Discovery überwacht die Zugriffsversuche von Benutzern auf diese Dienste sowohl über Browser als auch über Desktop-Anwendungen. Es überwacht zusätzlich die Versuche von Benutzern, über unverschlüsselte Verbindungen (z. B. mithilfe des HTTP-Protokolls) auf Cloud-Dienste zuzugreifen. Diese Funktion hilft Ihnen, die heimliche und unbefugte Verwendung von Cloud-Diensten zu erkennen und zu stoppen.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Security Center unter einer Lizenz für Kaspersky Next EDR Optimum oder Kaspersky Next XDR Expert aktiviert haben.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Endpoint Security 11.2 für Windows oder höher verwenden. Ältere Versionen der Sicherheitsanwendung erlauben Ihnen lediglich die Überwachung der Verwendung von Cloud-Diensten.

Sie können die Cloud Discovery-Funktion aktivieren und die Sicherheitsrichtlinien oder Profile auswählen, für die Sie die Funktion aktivieren möchten. Sie können die Funktion auch separat in jeder Sicherheitsrichtlinie oder jedem Profil aktivieren oder deaktivieren. Sie können den Zugriff auf Cloud-Dienste blockieren, auf welche die Benutzer nicht zugreifen dürfen.

Damit Sie den Zugriff auf unerwünschte Cloud-Dienste blockieren können, müssen die folgenden Voraussetzungen erfüllt sein:

- Sie verwenden Kaspersky Endpoint Security 11.2 für Windows oder höher. Ältere Versionen der Sicherheitsanwendung erlauben Ihnen lediglich die Überwachung der Verwendung von Cloud-Diensten.
- Sie haben eine Lizenz der Stufe "Kaspersky Next" erworben, in deren Rahmen Sie den Zugriff auf unerwünschte Cloud-Dienste blockieren können. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Next.

Das Cloud Discovery-Widget und die Berichte von Cloud Discovery enthalten Informationen über erfolgreiche und blockierte Zugriffsversuche auf Cloud-Dienste. Das Widget zeigt auch für jeden Cloud-Dienst die Risikostufe an. Kaspersky Security Center ruft die Informationen zur Verwendung von Cloud-Diensten von all den verwalteten Geräten ab, die nur durch jene Sicherheitsrichtlinien oder Sicherheitsprofile geschützt sind, für welche die Funktion aktiviert ist.

Cloud Discovery über das Widget aktivieren

Die Cloud Discovery-Funktion ruft die Informationen zur Verwendung von Cloud-Diensten von allen verwalteten Geräten ab, die nur durch jene Sicherheitsrichtlinien geschützt sind, für welche die Funktion aktiviert ist. Sie können Cloud Discovery nur für die Richtlinie von Kaspersky Endpoint Security für Windows aktivieren oder deaktivieren.

Es gibt zwei Möglichkeiten, die Cloud Discovery-Funktion zu aktivieren:

- Mithilfe des Cloud Discovery-Widgets.
- In den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows.

  Weitere Informationen zur Aktivierung von Cloud Discovery in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows im Abschnitt Cloud Discovery.

Beachten Sie, dass Sie Cloud Discovery nur in den Richtlinienparametern von Kaspersky Endpoint Security für Windows deaktivieren können.

Um Cloud Discovery zu aktivieren, müssen Sie für den Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen** über die Berechtigung **Schreiben** verfügen.

So aktivieren Sie die Cloud Discovery-Funktion mithilfe des Cloud Discovery-Widgets:

1. Wechseln Sie zu Kaspersky Security Center.
2. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
3. Klicken Sie im Widget **Cloud Discovery** auf **Aktivieren**.

Wenn Sie Kaspersky Endpoint Security für Windows Version 12.4 installiert haben, aktivieren Sie Cloud Discovery in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows. Weitere Informationen finden Sie im Abschnitt Cloud Discovery der Hilfe zu Kaspersky Endpoint Security für Windows.

Wenn Sie Kaspersky Endpoint Security für Windows bis Version 12.4 verwenden, aktualisieren Sie das Plug-in für Kaspersky Endpoint Security für Windows auf Version 12.5.

4. Wählen Sie im folgenden Fenster **Cloud Discovery aktivieren** die Sicherheitsrichtlinien aus, für welche Sie die Funktion aktivieren möchten, und klicken Sie anschließend auf **Aktivieren**.

   Die folgenden Richtlinieneinstellungen werden automatisch aktiviert: **Skript zum Interagieren mit Webseiten in den Web-Datenverkehr einbinden**, **Überwachen von Web-Sitzungen** und **Untersuchung verschlüsselter Verbindungen**.

Die Cloud Discovery-Funktion ist aktiviert und das Widget wurde dem Dashboard hinzugefügt.

Das Cloud Discovery-Widget zum Dashboard hinzufügen

Sie können das **Cloud Discovery-Widget** zum Dashboard hinzufügen, um die Nutzung von Cloud-Diensten auf verwalteten Geräten zu überwachen.

Um das Cloud Discovery-Widget zum Dashboard hinzuzufügen, müssen Sie das Recht **Schreiben** für den Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen** haben.

So fügen Sie das Cloud Discovery-Widget zum Dashboard hinzu:

1. Wechseln Sie zu Kaspersky Security Center.
2. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
3. Klicken Sie auf **Web-Widget hinzufügen oder wiederherstellen**.
4. Klicken Sie in der Liste der verfügbaren Widgets auf das Chevron-Symbol (>) neben der Kategorie **Andere**.
5. Wählen Sie das Widget **Cloud Discovery** aus und klicken Sie anschließend auf **Hinzufügen**.

   Wenn die Cloud Discovery-Funktion deaktiviert ist, befolgen Sie die Anweisungen im Abschnitt "Cloud Discovery über das Widget aktivieren".

Das ausgewählte Widget wird am Ende des Dashboards hinzugefügt.

Informationen zur Nutzung von Cloud-Diensten anzeigen

Sie können das **Cloud Discovery-Widget** anzeigen, das Informationen zu versuchten Zugriffen auf Cloud-Dienste zur Verfügung stellt. Das Widget zeigt auch für jeden Cloud-Dienst die Risikostufe an. Kaspersky Security Center ruft die Informationen zur Verwendung von Cloud-Diensten von all den verwalteten Geräten ab, die nur durch jene Sicherheitsprofile geschützt sind, für welche die Funktion aktiviert ist.

Stellen Sie vor dem Betrachten sicher, dass die folgenden Bedingungen erfüllt sind:

- Das Cloud Discovery-Widget wurde zum Dashboard hinzugefügt.
- Die Cloud Discovery-Funktion ist aktiviert.
- Sie verfügen über die Berechtigung **Lesen** für den Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen**.

So zeigen Sie das Cloud Discovery-Widget an:

1. Wechseln Sie zu Kaspersky Security Center.
2. Gehen Sie im Hauptmenü zu **Überwachung und Berichterstattung → Dashboard**.

   Das **Cloud Discovery** wird auf dem Dashboard angezeigt.
3. Wählen Sie auf der linken Seite des Widgets **Cloud Discovery** eine Kategorie für Cloud-Dienste aus.

   In der Tabelle auf der rechten Seite des Widgets werden für die ausgewählte Kategorie bis zu fünf Dienste angezeigt, auf welche die Benutzer am häufigsten versuchen zuzugreifen. Es werden sowohl erfolgreiche als auch blockierte Versuche gezählt.
4. Wählen Sie auf der rechten Seite des Widgets einen bestimmten Dienst aus.

   Die untere Tabelle enthält bis zu zehn Geräte, die am häufigsten versuchen, auf den Dienst zuzugreifen. In dieser Tabelle können Sie zwei Arten von Berichten erstellen: Bericht über erfolgreiche Zugriffsversuche und Bericht über blockierte Zugriffsversuche.

   Darüber hinaus können Sie in dieser Tabelle den Zugriff auf die Cloud-Dienste für Reihe von Geräten.

Das Widget zeigt die angeforderten Informationen an.

Im angezeigten Widget können Sie:

- Zum Abschnitt **Überwachung und Berichterstattung → Berichte** wechseln, um die Berichte von Cloud Discovery anzuzeigen.
- Den Zugriff auf den ausgewählten Cloud-Dienst blockieren oder erlauben.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Security Center unter einer Lizenz für Kaspersky Next EDR Optimum oder Kaspersky Next XDR Expert aktiviert haben.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Endpoint Security 11.2 für Windows oder höher verwenden. Ältere Versionen der Sicherheitsanwendung erlauben Ihnen lediglich die Überwachung der Verwendung von Cloud-Diensten.

Risikostufe eines Cloud-Dienstes

Cloud Discovery gibt für jeden Cloud-Dienst eine Risikostufe an. Anhand der Risikostufe können Sie Cloud-Dienste identifizieren, die nicht den Sicherheitsanforderungen Ihres Unternehmens entsprechen. Bei der Entscheidung, ob der Zugriff auf einen bestimmten Dienst blockiert werden muss, können Sie beispielsweise die Risikostufe des Dienstes berücksichtigen.

Die Risikostufe ist ein geschätzter Index, der weder etwas über die Qualität eines Cloud-Dienstes, noch über den Dienstanbieter aussagt. Die Risikostufe stellt lediglich eine Empfehlung von Kaspersky-Experten dar.

Die Risikostufen der Cloud-Dienste werden im Cloud Discovery-Widget und in der Liste aller überwachten Cloud-Dienste angezeigt.

Zugriffs auf unerwünschte Cloud-Dienste blockieren

Sie können den Zugriff auf Cloud-Dienste blockieren, auf welche die Benutzer nicht zugreifen sollen. Gleichermaßen können Sie den Zugriff auf zuvor gesperrte Cloud-Dienste erlauben.

Bei der Entscheidung, ob der Zugriff auf einen bestimmten Dienst blockiert werden soll, können Sie unter anderem die Risikostufe des Dienstes berücksichtigen.

Sie können den Zugriff auf Cloud-Dienste für eine Sicherheitsrichtlinie oder ein Profil blockieren oder erlauben.

Es gibt zwei Möglichkeiten, den Zugriff auf unerwünschte Cloud-Dienste zu blockieren:

- Mithilfe des Widgets von Cloud Discovery.

  In diesem Fall können Sie den Zugriff auf die Dienste einzeln sperren.

- In den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows.

  In diesem Fall können Sie den Zugriff auf die Dienste einzeln oder gleich für eine ganze Kategorie blockieren.

  Weitere Informationen zur Aktivierung von Cloud Discovery in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows im Abschnitt Cloud Discovery.

So blockieren oder erlauben Sie den Zugriff auf einen Cloud-Dienst mithilfe des Widgets:

1. Öffnen Sie das Cloud Discovery-Widget und wählen Sie anschließend den erforderlichen Cloud-Dienst aus.

2. Suchen Sie im Bereich **Top 10 der Geräte, die diesen Dienst verwenden** nach der Sicherheitsrichtlinie oder dem Profil, für die bzw. das Sie den Dienst blockieren oder zulassen möchten.

3. Führen Sie in der entsprechenden Zeile in der Spalte **Zugriffsstatus in Richtlinie oder Profil** einen der folgenden Schritte aus:

   - Um den Dienst zu blockieren, wählen Sie in der Dropdown-Liste die Option **Blockiert** aus.
   - Um den Dienst zu erlauben, wählen Sie in der Dropdown-Liste die Option **Zugelassen** aus.

4. Klicken Sie auf **Speichern**.

Der Zugriff auf den ausgewählten Dienst wird für die Sicherheitsrichtlinie oder das Profil gesperrt oder erlaubt.

Protokollieren der Aktivitäten der Kaspersky Security Center Web Console

Das Protokollieren der Aktivitäten der Kaspersky Security Center Web Console hilft Ihnen dabei, die Ursachen für Fehler bei der Programmausführung zu finden. Wenn Sie Kontakt mit dem Technischen Support von Kaspersky aufnehmen, um einen Fehler in der Ausführung der Kaspersky Security Center Web Console zu lösen, fordern die Experten des Technischen Supports Sie eventuell auf, ihnen Log-Dateien der Kaspersky Security Center Web Console zuzusenden. Die Log-Dateien von Kaspersky Security Center Web Console werden während des gesamten Betriebs des Programms im <Installationsverzeichnis der Kaspersky Security Center Web Console> im Unterordner /logs gespeichert. Die Log-Dateien werden nicht automatisch an die Experten des Technischen Supports von Kaspersky gesendet.

Um das Protokollieren der Aktivitäten der Kaspersky Security Center Web Console zu aktivieren,

Wählen Sie die Option **Aktivieren Sie die Protokollierung der Aktivitäten von Kaspersky Security Center Web Console** im Fenster **Verbindungseinstellungen für Kaspersky Security Center Web Console** des Installationsassistenten für Kaspersky Security Center Web Console.

Die Log-Dateien werden im Textformat gespeichert.

Die Namen der Log-Dateien setzen sich wie folgt zusammen: logs-<Komponentenname>.<Gerätename>-<Nummer der Dateirevision>.YYYY-MM-DD, wobei:

- <Komponentenname> der Name der Komponente von Kaspersky Security Center oder der Name des Verwaltungs-Plug-ins von Kaspersky Security Center Web Console ist.
- <Gerätname> der Name des Geräts ist, auf dem die Komponente <Komponentenname> ausgeführt wird.
- <Nummer der Dateirevision> die Nummer der Log-Datei ist, die für die Komponente <Komponentenname>, die auf <Hostname> ausgeführt wird, erstellt wurde. innerhalb eines Tages können mehrere Log-Dateien für die gleiche Komponente <Komponentenname> und <Gerätename> erstellt werden. Die Maximalgröße einer Log-Datei beträgt 50 Megabyte (MB). Bei Erreichen der Maximalgröße wird eine neue Log-Datei erstellt. Die <Nummer der Dateirevision> der neuen Log-Datei wird um 1 inkrementiert.
- YYYY, MM und DD sind das Jahr, der Monat und der Tag, an dem die Log-Datei erstmals erstellt wurde. Zu Beginn eines neuen Tages wird eine neue Log-Datei erstellt.

Integration von Kaspersky Security Center und weiteren Lösungen

Dieser Abschnitt beschreibt, wie Sie den Zugriff von Kaspersky Security Center Web Console auf andere Kaspersky-Anwendungen, wie Kaspersky Managed Detection and Response, konfigurieren. Außerdem wird in diesem Abschnitt beschrieben, wie der Export in SIEM-Systeme konfiguriert wird.

Hintergrundverbindung herstellen

Damit die Kaspersky Security Center Web Console ihre Hintergrundaufgaben ausführen kann, müssen Sie eine Hintergrundverbindung zwischen der Kaspersky Security Center Web Console und dem Administrationsserver herstellen. Sie können diese Verbindung nur dann herstellen, wenn Ihr Benutzerkonto die Berechtigung **Objekt-ACL ändern** im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** besitzt.

Wenn Sie das Plug-in von Kaspersky Endpoint Security für Windows 12.6 installieren oder wenn Sie das Plug-in von Kaspersky Endpoint Security für Windows von einer Version, früher als 11.7, aktualisieren und dabei noch keine Background-Verbindung hergestellt wurde, wird eine Benachrichtigung angezeigt, dass Sie eine Background-Verbindung herstellen müssen. Außerdem müssen Sie dem Dienstkonto die Berechtigungen für den Funktionsbereich **Allgemeine Funktionen: Vorgänge auf dem Administrationsserver** zuweisen.

So stellen Sie eine Hintergrundverbindung her:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Integration**.
2. Setzen Sie im Abschnitt **Integration** den Umschalter zum Herstellen einer Background-Verbindung auf die Position **Background-Verbindung für die Integration Aktiviert**.
3. Klicken Sie im folgenden Abschnitt **Background-Verbindung aktivieren** auf die Schaltfläche **OK**.

Die Hintergrundverbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver wird hergestellt. Der Administrationsserver erstellt für die Hintergrundverbindung ein Benutzerkonto, das als Dienstkonto verwendet wird, um die Interaktion zwischen Kaspersky Security Center und einer anderen Lösung oder Anwendung von Kaspersky aufrechtzuerhalten. Der Name des Dienstkontos enthält den Präfix "NWCSvcUser".

Aus Sicherheitsgründen ändert der Administrationsserver das Kennwort des Dienstkontos automatisch alle 30 Tage. Das Dienstkonto kann nicht manuell gelöscht werden. Der Administrationsserver löscht dieses Konto automatisch, wenn Sie die dienstübergreifende Verbindung deaktivieren. Der Administrationsserver erstellt für jede Verwaltungskonsole ein separates Dienstkonto und weist alle Dienstkonten der Sicherheitsgruppe mit dem Namen "ServiceNwcGroup" zu. Der Administrationsserver erstellt diese Sicherheitsgruppe automatisch während der Installation von Kaspersky Security Center. Diese Sicherheitsgruppe kann nicht manuell gelöscht werden.

Ereignisse in SIEM-Systeme exportieren

Dieser Abschnitt beschreibt, wie Sie den Export von Ereignissen in ein SIEM-System konfigurieren.

Ereignisexport in SIEM-Systeme konfigurieren

Kaspersky Security Center ermöglicht die Konfiguration mit einer der folgenden Methoden: Export in ein beliebiges SIEM-System mit Syslog-Format; Export in die SIEM-Systeme QRadar, Splunk, ArcSight mit LEEF- und CEF-Format; direkter Export von Ereignissen in SIEM-Systeme aus der Datenbank von Kaspersky Security Center. Nach Abschluss dieses Szenarios sendet der Administrationsserver Ereignisse automatisch an das SIEM-System.

Erforderliche Vorrausetzungen

Bevor Sie mit der Konfiguration des Ereignisexports in die Kaspersky Security Center beginnen:

- Erfahren Sie mehr über die Exportmethoden.
- Stellen Sie sicher, dass Sie die Werte der Systemeinstellungen kennen.

> Sie können die Schritte in diesem Szenario in beliebiger Reihenfolge ausführen.

Der Prozess des Ereignisexports in SIEM-Systeme umfasst die folgenden Schritte:

- **Konfigurieren des SIEM-Systems, so dass es Ereignisse aus Kaspersky Security Center empfängt**

  Anleitung: Einstellungen für den Ereignisexport in das SIEM-System

- **Auswählen der Ereignisse, die Sie in das SIEM-System exportieren möchten:**

  Anleitung:

  - Verwaltungskonsole: Ereignisse einer Kaspersky-Anwendung für den Export im Syslog-Format markieren, Allgemeine Ereignisse für den Export im Syslog-Format markieren
  - Kaspersky Security Center Web Console: Ereignisse einer Kaspersky-Anwendung für den Export im Syslog-Format markieren, Allgemeine Ereignisse für den Export im Syslog-Format markieren

- **Konfigurieren des Ereignisexports in ein SIEM-System unter Verwendung einer der folgenden Methoden:**

  - Mittels der Protokolle TCP, UDP oder TLS over TCP.

    Anleitung:

    - Verwaltungskonsole: Export von Ereignissen in SIEM-Systeme konfigurieren
    - Kaspersky Security Center Web Console: Export von Ereignissen in SIEM-Systeme konfigurieren

  - Mittels direktem Ereignisexport aus der Datenbank von Kaspersky Security Center (In der Datenbank von Kaspersky Security Center ist eine Auswahl an öffentlichen Ansichten verfügbar. Die Beschreibung dieser Ansichten finden Sie im Dokument klakdb.chm).

Ergebnisse

Nach der Konfiguration des Ereignisexports in ein SIEM-System, können Sie sich die Exportergebnisse ansehen, wenn Sie Ereignisse ausgewählt haben, die Sie exportieren wollen.

Vorläufige Bedingungen

Bei den Einstellungen für den automatischen Ereignisexport in Kaspersky Security Center müssen einige Einstellungen des SIEM-Systems angegeben werden. Es ist empfehlenswert, diese Einstellungen im Voraus zu bestimmen, damit die Einstellungen für Kaspersky Security Center vorbereitet werden können.

Für die Einstellungen des automatischen Ereignisexports ins SIEM-System müssen die Werte der folgenden Einstellungen bekannt sein:

- **Serveradresse des SIEM-Systems**

  IP-Adresse des Servers, auf dem das verwendete SIEM-System installiert ist. Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

- **Serverport des SIEM-Systems**

  Port, über den eine Verbindung zwischen Kaspersky Security Center und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

- **Protokoll**

  Das Protokoll, das für die Übertragung von Daten aus Kaspersky Security Center ins SIEM-System verwendet wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

Über Ereignisse in Kaspersky Security Center

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert. Sie können diese Informationen in externe SIEM-Systeme exportieren. Der Export von Informationen über Ereignisse in externen SIEM-Systeme ermöglicht den Administratoren der SIEM-Systeme, auf die Ereignisse des Sicherheitssystems, die auf den verwalteten Geräten oder in den Administrationsgruppen auftreten, operativ zu reagieren.

Ereignistypen

In Kaspersky Security Center existieren die folgenden Ereignistypen:

- Allgemeine Ereignisse. Diese Ereignisse kommen in allen verwalteten Kaspersky-Anwendungen vor. Als allgemeines Ereignis gilt beispielsweise das Ereignis Virenangriff. Allgemeine Ereignisse haben eine streng definierte Syntax und Semantik. Allgemeine Ereignisse werden beispielsweise in Berichten und auf Dashboards verwendet.

- Spezifische Ereignisse für verwaltete Kaspersky-Anwendungen. Jede verwaltete Kaspersky-Anwendung hat eine eigene Auswahl von Ereignissen.

Quellen von Ereignissen

Ereignisse können von den folgenden Programmen generiert werden:

- Komponenten von Kaspersky Security Center:
  - Administrationsserver
  - Administrationsagent
  - iOS MDM-Server
- Verwaltete Kaspersky-Anwendungen

  Weitere Informationen zu den Ereignissen, die von verwalteten Kaspersky-Programmen generiert werden, finden Sie in der Dokumentation des entsprechenden Programms.

Sie können die vollständige Liste der Ereignisse anzeigen, die von einer Anwendung auf der Registerkarte **Konfiguration von Ereignissen** in der Anwendungsrichtlinie generiert werden können. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen.

Ereigniskategorie von Ereignissen

Jedes Ereignis hat eine eigene Ereigniskategorie. Je nach den Bedingungen des Auftretens, können dem Ereignis verschiedene Ereigniskategorien zugewiesen werden. Es sind vier Ereigniskategorien verfügbar:

- *Kritisches Ereignis* – ein Ereignis, das auf das Auftreten eines kritischen Problems hinweist, das zu Datenverlust, einer Ausführungsstörung oder einem kritischen Fehler führen kann.
- *Funktionsfehler* – das Ereignis, das auf das Auftreten eines ernsten Problems, Fehlers oder einer Störung hinweist, welches während der Ausführung des Programms oder der Prozedur entstanden ist.
- *Warnung* – ein nicht unbedingt ernstes dem Ereignis, das jedoch auf die potentiell mögliche Entstehung eines Problems in der Zukunft hinweist. Meistens gehört die Mehrzahl der Ereignisse zu den Warnungen, wenn nach ihrem Auftreten die Ausführung der Anwendung ohne Datenverlust oder eingeschränkter Funktionalität wiederhergestellt werden kann.
- *Infomeldung* – Ereignis, das zwecks Information über das erfolgreiche Ausführen einer Operation, die korrekte Ausführung des Programms oder den Abschluss einer Prozedur auftritt.

Für jedes Ereignis ist die Speicherdauer festgelegt, die in Kaspersky Security Center angezeigt oder geändert werden kann. Einige Ereignisse werden nicht standardmäßig in der Datenbank des Administrationsservers gespeichert, da die für sie definierte Speicherdauer gleich Null ist. In externe Systeme können nur jene Ereignisse exportieren, die mindestens einen Tag in der Administrationsserver-Datenbank gespeichert werden.

Über den Ereignisexport

Sie können den Ereignisexport innerhalb zentralisierten Systemen verwenden, die sich mit Fragen der Sicherheit auf organisatorischer und technischer Ebene und der Überwachung des Sicherheitssystems beschäftigen sowie Daten aus verschiedenen Lösungen konsolidieren. Dazu gehören SIEM-Systeme, die eine Analyse der Warnungen der Sicherheitssysteme und Ereignisse der Netzwerkhardware und Anwendungen im Echtzeitbetrieb gewährleisten, sowie Security Operation Center (SOC).

Diese Systeme erhalten Daten aus vielen Quellen, einschließlich Netzwerke, Sicherheitssysteme, Server, Datenbanken und Anwendungen. Ferner gewährleisten SIEM-Systeme eine Zusammenfassung der bearbeiteten Daten, damit Sie keine kritischen Ereignisse überspringen können. Außerdem führen diese Systeme eine automatische Analyse der verbundenen Ereignisse und der Alarme zur Benachrichtigung der Administratoren über Fragen des Sicherheitssystems, die eine sofortige Entscheidung fordern, durch. Die Benachrichtigungen können im Indikatorbereich angezeigt oder über dritte Kanäle, beispielsweise E-Mail, versendet werden.

Am Ablauf des Ereignisexports aus Kaspersky Security Center in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Security Center – und der Empfänger der Ereignisse – das SIEM-System. Für einen erfolgreichen Ereignisexport müssen die Einstellungen sowohl im verwendeten SIEM-System als auch in Kaspersky Security Center angepasst werden. Die Reihenfolge der Einstellungen hat keine Bedeutung: Sie können zuerst den Versand der Ereignisse in Kaspersky Security Center und dann das Empfangen der Ereignisse im SIEM-System anpassen oder umgekehrt.

Methoden für den Versand von Ereignissen aus Kaspersky Security Center

Es gibt drei Methoden für den Versand von Ereignisse aus Kaspersky Security Center in die externen Systeme:

- Versand von Ereignissen gemäß dem Protokoll Syslog in ein beliebiges SIEM-System

  Gemäß dem Protokoll Syslog können beliebige Ereignisse, die auf dem Kaspersky Security Center Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, übertragen werden. Das Syslog-Protokoll ist ein Standardprotokoll für das Aufzeichnen von Nachrichten. Sie können es für den Export von Ereignissen ein beliebiges SIEM-System verwenden.

  Zu diesem Zweck müssen Sie die Ereignisse markieren, die Sie an das SIEM-System weiterleiten möchten. Die Ereignisse können Sie in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console markieren. Es werden nur markierte Ereignisse an das SIEM-System weitergeleitet. Wenn Sie nichts markiert haben, werden keine Ereignisse weitergeleitet.

- Versand von Ereignissen gemäß den Protokollen CEF und LEEF in die Systeme QRadar, Splunk und ArcSight

  Sie können die Protokolle CEF und LEEF verwenden, um allgemeine Ereignisse zu exportieren. Die Protokolle CEF und LEEF sind im Gegensatz zum Protokoll Syslog nicht universell. Stattdessen werden alle allgemeinen Ereignisse exportiert. Um Ereignisse von Kaspersky Security Center in Ereignisse im CEF- und LEEF-Format zu konvertieren, können Sie die Datei siem_conversion_rules.xml verwenden. Diese Datei enthält die Liste der Ereignisattribute von Kaspersky Security Center und deren entsprechenden Ereignisattribute im CEF- und LEEF-Format. Zusätzlich enthält die Datei "siem_conversion_rules.xml" Regeln zum Generieren von Nachrichten zu den entsprechenden Ereignissen. Diese Datei ist im Lieferumfang von Kaspersky Security Center enthalten.

  Anders als das Syslog-Protokoll sind das CEF- und das LEEF-Protokoll nicht universell. CEF und LEEF sind für die entsprechenden SIEM-Systeme (QRadar, Splunk und ArcSight) vorgesehen. Wenn Sie daher Ereignisse über eines dieser Protokolle exportieren, verwenden Sie den erforderlichen Parser im SIEM-System.

- Direkt aus der Datenbank von Kaspersky Security Center in ein beliebiges SIEM-System

  Diese Methode für den Ereignisexport kann für das Empfangen von Ereignissen direkt aus den öffentlichen Ansichten der Datenbank mithilfe von SQL-Abfragen verwendet werden. Die Ausführungsergebnisse der Anfrage werden in einer xml-Datei gespeichert und können als Eingangsdaten für das externe System verwendet werden. Nur Ereignisse, die in öffentlichen Ansichten verfügbar sind, können direkt aus der Datenbank exportiert werden.

Empfangen von Ereignissen im SIEM-System

Das SIEM-System muss die von Kaspersky Security Center übertragenen Ereignisse korrekt übernehmen und analysieren. Dazu müssen die Einstellungen des SIEM-Systems angepasst werden. Die Konfiguration hängt vom verwendeten speziellen SIEM-System ab. Es gibt jedoch eine Anzahl von allgemeinen Schritten in der Konfiguration aller SIEM-Systeme, etwa die Konfiguration des Empfängers und des Parsers.

Über das Konfigurieren des Ereignisexports in ein SIEM-System

Am Ablauf des Ereignisexports aus Kaspersky Security Center in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Security Center – und der Empfänger der Ereignisse – das SIEM-System. Der Ereignisexport wird im verwendeten SIEM-System und in Kaspersky Security Center angepasst.

Die Einstellungen, die im SIEM-System vorgenommen werden, sind vom System abhängig, das Sie verwenden. Im Allgemeinen müssen für alle SIEM-Systeme der Empfänger der Nachrichten und, falls erforderlich, der Nachrichtenparser angepasst werden, damit die erhaltenen Nachrichten auf die Felder verteilt werden können.

Einstellungen des Empfängers der Nachrichten

Für das SIEM-Systems muss der Empfänger für den Erhalt der Ereignisse, die von Kaspersky Security Center gesendet werden, angepasst werden. Im Allgemeinen müssen im SIEM-System die folgenden Einstellungen angegeben werden:

- **Exportprotokoll oder Typ der Eingangsdaten**

  Dies ist das Protokoll zum Übertragen von Nachrichten, beispielsweise UDP. Das Protokoll muss das dasselbe Protokoll sein, das Sie in Kaspersky Security Center angegeben haben.

- **Port**

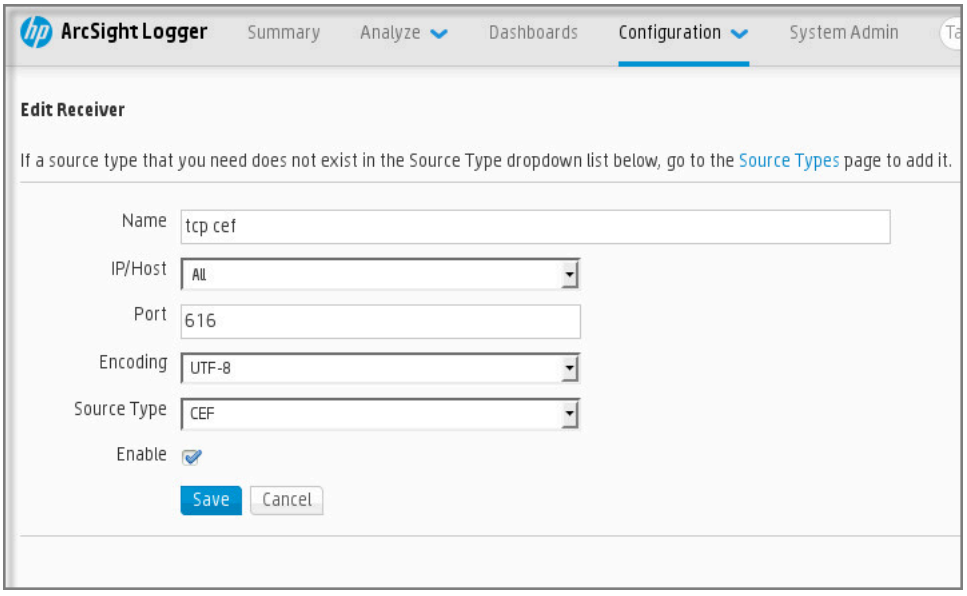
  Port für die Verbindung mit Kaspersky Security Center. Es muss derselbe Port angegeben werden, der in Kaspersky Security Center für die Übertragung der Ereignisse ausgewählt war.

- **Übertragungsprotokoll der Nachrichten oder Typ der Quelldaten**

  Protokoll für den Ereignisexport in das SIEM-System Es kann eines der Standardprotokolle sein: Syslog, CEF oder LEEF. Das SIEM-System wählt den Nachrichtenparser gemäß dem angegebenen Protokoll aus.

Je nachdem, welches SIEM-System Sie verwendetem, kann es erforderlich sein, erweiterte Einstellungen für den Empfänger der Nachrichten anzugeben.

Auf der unteren Abbildung dienen die Einstellungen des Empfängers in ArcSight als Beispiel.



Einstellungen des Empfängers in ArcSight

Nachrichtenparser

Die exportierten Ereignisse werden in Form von Nachrichten an das SIEM-System übergeben. Dann wird für diese Nachrichten der Parser verwendet, damit die Informationen über die Ereignisse entsprechend ins SIEM-System übergeben werden. Die Nachrichtenparser sind im SIEM-System integriert und werden für die Aufteilung der Nachrichten in Felder wie Nachrichten-ID, Signifikanz, Beschreibung und Parameter verwendet. Daraufhin hat das SIEM-System die Möglichkeit, die Ereignisse, die aus Kaspersky Security Center empfangen werden, so zu verarbeiten, dass sie in der Datenbank des SIEM-Systems gespeichert werden.

Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren

Nach der Aktivierung des automatischen Ereignisexports müssen Sie auswählen, welche Ereignisse ins externe SIEM-System exportiert werden sollen.

Sie können den Ereignisexport in das Syslog-Format in ein externes System gemäß einer der folgenden Bedingungen anpassen:

- Allgemeine Ereignisse markieren. Wenn Sie die zu exportierenden Ereignisse in der Richtlinie, in den Einstellungen eines Ereignisses oder in den Einstellungen des Administrationsservers markieren, erhält das SIEM-System die ausgewählten Ereignisse, die in allen Anwendungen auftreten, die von der Richtlinie verwaltet werden. Falls die zu exportierenden Ereignisse in der Richtlinie ausgewählt worden sind, ist es unmöglich, diese für eine einzelne Anwendung, die von dieser Richtlinie verwaltet wird, umzudefinieren.

- Ereignisse für eine verwaltete Anwendung markieren. Wenn Sie die zu exportierenden Ereignisse für eine verwaltete Anwendungen auf einem verwalteten Gerät markieren, werden nur Ereignisse in das SIEM-System übertragen, die in dieser Anwendung aufgetreten sind.

Über das Markieren von Ereignissen zum Export in SIEM-Systeme im Syslog-Format

Nach der Aktivierung des automatischen Ereignisexports müssen Sie auswählen, welche Ereignisse ins externe SIEM-System exportiert werden sollen.

Sie können den Ereignisexport in das Syslog-Format in ein externes System gemäß einer der folgenden Bedingungen anpassen:

- Allgemeine Ereignisse markieren. Wenn Sie die zu exportierenden Ereignisse in der Richtlinie, in den Einstellungen eines Ereignisses oder in den Einstellungen des Administrationsservers markieren, erhält das SIEM-System die ausgewählten Ereignisse, die in allen Anwendungen auftreten, die von der Richtlinie verwaltet werden. Falls die zu exportierenden Ereignisse in der Richtlinie ausgewählt worden sind, ist es unmöglich, diese für eine einzelne Anwendung, die von dieser Richtlinie verwaltet wird, umzudefinieren.

- Ereignisse für eine verwaltete Anwendung markieren. Wenn Sie die zu exportierenden Ereignisse für eine verwaltete Anwendung auf einem verwalteten Gerät markieren, werden nur Ereignisse in das SIEM-System übertragen, die in dieser Anwendung aufgetreten sind.

Ereignisse von Kaspersky-Anwendungen zum Export im Syslog-Format markieren

Wenn Sie Ereignisse exportieren möchten, die in einer bestimmten verwalteten Anwendung, welche auf den verwalteten Geräten installiert ist, auftreten, markieren Sie in der Anwendungsrichtlinie die Ereignisse für den Export. In diesem Fall werden die markierten Ereignisse von allen Geräten, die sich im Gültigkeitsbereich der Richtlinie befinden, exportiert.

Um zu exportierende Ereignisse für eine bestimmte verwaltete Anwendung zu markieren, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie der Anwendung, für die Sie die Ereignisse markieren möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.
3. Gehen Sie zum Abschnitt **Konfiguration von Ereignissen**.
4. Aktivieren Sie die Kontrollkästchen neben den Ereignissen, die Sie in ein SIEM-System exportieren möchten.
5. Klicken Sie auf die Schaltfläche **Für den Export in ein SIEM-System mittels Syslog auswählen**.

   Außerdem können Sie im Abschnitt **Ereignisregistrierung**, welcher sich durch Anklicken eines Ereignislinks öffnet, ein Ereignis für den Export in ein SIEM-System markieren.
6. In der Spalte **Syslog** des Ereignisses, oder der Ereignisse, die Sie für den Export in ein SIEM-System markiert haben, erscheint ein Häkchen (✓).
7. Klicken Sie auf die Schaltfläche **Speichern**.

Die markierten Ereignisse aus der verwalteten Anwendung sind für den Export in ein SIEM-System vorbereitet.

Sie können markieren, welche Ereignisse für ein bestimmtes verwaltetes Gerät in ein SIEM-System exportiert werden sollen. Falls bereits früher exportierte Ereignisse in einer Anwendungsrichtlinie markiert wurden, können Sie die markierten Ereignisse für ein verwaltetes Gerät nicht neu definieren.

Um zu exportierende Ereignisse für ein verwaltetes Gerät zu markieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.
2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des benötigten Geräts.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.
3. Gehen Sie zum Abschnitt **Programme**.
4. Klicken Sie in der Liste der Anwendungen auf den Link mit dem Namen der benötigten Anwendung.
5. Wechseln Sie zum Abschnitt **Konfiguration von Ereignissen**.
6. Aktivieren Sie die Kontrollkästchen neben den Ereignissen, die Sie nach SIEM exportieren möchten.
7. Klicken Sie auf die Schaltfläche **Für den Export in ein SIEM-System mittels Syslog auswählen**.

   Außerdem können Sie im Abschnitt **Ereignisregistrierung**, welcher sich durch Anklicken eines Ereignislinks öffnet, ein Ereignis für den Export in ein SIEM-System markieren.
8. In der Spalte **Syslog** des Ereignisses, oder der Ereignisse, die Sie für den Export in ein SIEM-System markiert haben, erscheint ein Häkchen (✓).

Bei konfiguriertem Export in ein SIEM-System sendet der Administrationsserver ab jetzt die ausgewählten Ereignisse an das SIEM-System.

Allgemeine Ereignisse zum Export im Syslog-Format markieren

Sie können allgemeine Ereignisse markieren, die der Administrationsserver unter Verwendung des Syslog-Formats in SIEM-Systeme exportiert.

So markieren Sie Ereignisse für den Export in ein SIEM-System:

1. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).
   - Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile** → und klicken Sie anschließend auf den Link einer Richtlinie.

2. Wechseln Sie im daraufhin geöffneten Fenster auf die Registerkarte **Konfiguration von Ereignissen**.

3. Klicken Sie auf die Schaltfläche **Für den Export in ein SIEM-System mittels Syslog auswählen**.

   Außerdem können Sie im Abschnitt **Ereignisregistrierung**, welcher sich durch Anklicken eines Ereignislinks öffnet, ein Ereignis für den Export in ein SIEM-System markieren.

4. In der Spalte **Syslog** des Ereignisses, oder der Ereignisse, die Sie für den Export in ein SIEM-System markiert haben, erscheint ein Häkchen ( ).

Bei konfiguriertem Export in ein SIEM-System sendet der Administrationsserver ab jetzt die ausgewählten Ereignisse an das SIEM-System.

Über das Exportieren von Ereignissen mittels der Formate CEF und LEEF

Die CEF- und LEEF-Formate können verwendet werden, um allgemeine Ereignisse und Ereignisse, die von Kaspersky-Anwendungen an den Administrationsserver übertragen werden, in SIEM-Systeme zu exportieren. Der Satz der zu exportierenden Ereignisse ist vordefiniert, es gibt keine Möglichkeit, die zu exportierenden Ereignisse auszuwählen. Bevor Ereignisse aus Kaspersky Security Center an ein SIEM-System (QRadar, ArcSight oder Splunk) übertragen werden können, müssen diese Ereignisse in das CEF- oder LEEF-Format konvertiert werden. Dies geschieht unter Verwendung der Regeln, die in der Datei siem_conversion_rules.xml enthalten sind.

Das Exportformat kann abhängig vom verwendeten SIEM-System ausgewählt werden. In der folgenden Tabelle sind die SIEM-Systeme und die ihnen entsprechenden Exportformate angeführt.

Formate für den Ereignisexport in ein SIEM-System

SIEM-System	Exportformat
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) ist ein spezielles Format für Ereignisprotokollierung in IBM Security QRadar SIEM. QRadar kann Ereignisse, die gemäß dem LEEF-Protokoll übergeben werden, sammeln, identifizieren und bearbeiten. Für das LEEF-Protokoll muss die UTF-8-Kodierung verwendet werden. Ausführlicheren Informationen über das LEEF-Protokoll finden Sie im IBM Knowledge Center.

- CEF ist ein Standard der Verwaltung vom Typ "offenes Protokoll", der die Kompatibilität der Informationen des Sicherheitssystems verschiedener Netzwerkgeräte und Apps verbessert. Das CEF-Protokoll ermöglicht die Verwendung eines allgemeinen Formats für das Ereignisprotokoll, damit die Managementsysteme für Unternehmen die Daten für die Analyse problemlos abrufen und zusammenfassen können. Für das CEF-Protokoll muss die UTF-8-Kodierung verwendet werden.

Automatischer Export bedeutet, dass Kaspersky Security Center die allgemeinen Ereignisse ins SIEM-System sendet. Der automatische Export der Ereignisse beginnt sofort nach der Aktivierung. In diesem Abschnitt ist der Ablauf zur Aktivierung des automatischen Exports von Ereignissen beschrieben.

Ereignisse in das CEF- oder LEEF-Format konvertieren

Bevor Ereignisse aus Kaspersky Security Center an ein SIEM-System (QRadar, ArcSight oder Splunk) übertragen werden können, müssen diese Ereignisse in das CEF- oder LEEF-Format konvertiert werden. Dies geschieht unter Verwendung der Regeln, die in der Datei "siem_conversion_rules.xml" enthalten sind. Diese Datei ist im Lieferumfang von Kaspersky Security Center enthalten.

Die Datei "siem_conversion_rules.xml" enthält die vordefinierten Interpretationsregeln zum Konvertieren von Ereignissen in das CEF- und LEEF-Format. Wenn Sie zusätzliche Regeln für die Ereignisinterpretation verwenden möchten, können Sie diese der Datei manuell hinzufügen.

Die Datei "siem_conversion_rules.xml" enthält die folgenden Abschnitte:

- `<product name="SP_QRADAR" vendor="IBM">`

  Dieser Abschnitt enthält Regeln zum Erstellen von Ereignissen im LEEF-Format, die in ein SIEM-System von QRadar exportiert werden können.

- [[<product name="SP_ARCSIGHT" vendor="HP">]]

  Dieser Abschnitt enthält Regeln zum Erstellen von Ereignissen im CEF-Format, die in SIEM-Systeme von ArcSight oder Splunk exportiert werden können.

Jeder Abschnitt besitzt den Unterabschnitt `<common>`, in dem sich die Ereignisattribute von Kaspersky Security Center und deren entsprechenden Ereignisattribute im LEEF-Format befinden. Diese gemeinsamen Attribute werden für alle Arten von Ereignissen verwendet, die exportiert werden können.

Zusätzlich besitzt jeder Abschnitt den Unterabschnitt `<event>`. Jeder `<event>`-Unterabschnitt enthält weitere Attribute, die den Attributen des Abschnitts `<common>` hinzugefügt werden.

Sie können der Datei "siem_conversion_rules.xml" eine neue Regel zur Ereignisgenerierung manuell hinzufügen.

So fügen Sie eine neue Regel zur Ereignisgenerierung hinzu:

1. Fügen Sie dem Abschnitt `<product name="SP_QRADAR" vendor="IBM">` oder `<product name="SP_ARCSIGHT" vendor="HP">` den neuen Unterabschnitt `<event>` hinzu und geben Sie anschließend bei Bedarf die weiteren Ereignisattribute ein.

2. Wenn ein Ereignis nur aus gemeinsamen Attributen besteht, bleibt der Unterabschnitt `<event>` leer.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Über das Exportieren von Ereignissen im Syslog-Format

Gemäß dem Syslog-Format können Ereignisse, die auf dem Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, ins SIEM-System exportiert werden.

Syslog ist ein Standardprotokoll zur Registrierung von Nachrichten. Dieses Protokoll ermöglicht, die Software, in der die Nachrichten generiert werden, das System, in dem die Nachrichten gespeichert werden, und die Software, in der die Analysen und die Berichterstellung für die Nachrichten ausgeführt wird, zu trennen. Jeder Nachricht wird der Code des Geräts, der den Typ der Software angibt, mit dessen Hilfe die Nachricht erstellt wurde, und die Signifikanz zugewiesen.

Das Syslog-Format wird in den Dokumenten "Request for Comments" (RFC) definiert, die von der Internet Engineering Task Force veröffentlicht werden. Der Standard RFC 5424 wird für den Ereignisexport aus Kaspersky Security Center in externe Systeme verwendet.

n Kaspersky Security Center können Sie den Ereignisexport in externe Systeme gemäß dem Syslog-Format anpassen.

Der Ablauf des Exports besteht aus zwei Schritten:

1. Aktivierung des automatischen Ereignisexports. In diesem Schritt werden die Einstellungen von Kaspersky Security Center so angepasst, dass der Versand von Ereignissen ins SIEM-System ausgeführt werden kann. Der Versand von Ereignissen aus Kaspersky Security Center beginnt sofort nach der Aktivierung des automatischen Exports.

2. Auswahl der Ereignisse, die ins externe System exportiert werden sollen. In diesem Schritt müssen Sie auswählen, welche Ereignisse ins SIEM-System exportiert werden sollen.

Konfiguration von Kaspersky Security Center für den Export an ein SIEM-System

Um Ereignisse an ein SIEM-System zu exportieren müssen Sie den Exportprozess in Kaspersky Security Center Web Console konfigurieren.

Bevor Ereignisse aus Kaspersky Security Center an ein SIEM-System (QRadar, ArcSight oder Splunk) übertragen werden können, müssen diese Ereignisse in das CEF- oder LEEF-Format konvertiert werden. Dies geschieht unter Verwendung der Regeln, die in der Datei siem_conversion_rules.xml enthalten sind.

So konfigurieren Sie den Export in SIEM-Systeme in Kaspersky Security Center Web Console:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **SIEM-Export** aus.

3. Klicken Sie auf den Link **Einstellungen**.

   Der Abschnitt **Einstellungen exportieren** wird geöffnet.

4. Legen Sie im Abschnitt **Einstellungen exportieren** die Einstellungen fest:

   - **Serveradresse des SIEM-Systems**

     IP-Adresse des Servers, auf dem das verwendete SIEM-System installiert ist. Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

   - **Port des SIEM-Systems**

     Port, über den eine Verbindung zwischen Kaspersky Security Center und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

   - **Protokoll**

     Wählen Sie das Übertragungsprotokoll für Nachrichten ins SIEM-System aus. Sie können das TCP-, UDP- oder TLS-over-TCP-Protokoll auswählen.

     Wenn Sie das Protokoll TLS over TCP auswählen, geben Sie die folgenden TLS-Einstellungen an:

     - **Authentifizierung des Servers**

In dem Feld **Authentifizierung des Servers** können Sie die **Vertrauenswürdige Zertifikate** oder Werte der **SHA-Fingerabdrücke** auswählen:

- **Vertrauenswürdige Zertifikate**. Sie können eine vollständige Zertifikatkette (einschließlich des Root-Zertifikats) von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority – CA) abrufen und diese Datei in Kaspersky Security Center hochladen. Kaspersky Security Center prüft, ob die Zertifikatkette des SIEM-Servers auch von einer vertrauenswürdigen CA signiert ist oder nicht.

  Um ein vertrauenswürdiges Zertifikat hinzuzufügen, klicken Sie auf die Schaltfläche **CA-Zertifikatsdatei auswählen** und laden Sie anschließend das Zertifikat hoch.

- **SHA-Fingerabdrücke**. Sie können SHA1-Fingerabdrücke der vollständigen Zertifikatkette des SIEM-Systems (einschließlich des Root-Zertifikats) in Kaspersky Security Center angeben. Um einen SHA1-Fingerabdruck hinzuzufügen, geben Sie ihn in das Feld **Fingerabdrücke** ein und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

Durch Verwendung der Einstellung **Client-Authentifizierung hinzufügen** können Sie ein Zertifikat generieren, um Kaspersky Security Center zu authentifizieren. Infolge dessen verwenden Sie ein selbstsigniertes Zertifikat, das von Kaspersky Security Center ausgestellt wurde. In diesem Fall können Sie sowohl ein vertrauenswürdiges Zertifikat als auch einen SHA-Fingerabdruck verwenden, um den SIEM-Systemserver zu authentifizieren.

- **Name/alternativen Namen des Antragstellers hinzufügen**

  Der Antragstellername ist ein Domänenname, für den das Zertifikat empfangen wird. Kaspersky Security Center kann keine Verbindung zu dem SIEM-System-Server herstellen, wenn der Domänenname des SIEM-System-Servers nicht mit dem Antragstellernamen des Zertifikats des SIEM-System-Servers übereinstimmt. Der SIEM-Systemserver kann jedoch seinen Domänennamen ändern, wenn sich der Name im Zertifikat geändert hat. In diesem Fall können Sie die Antragstellernamen im Feld **Name/alternativen Namen des Antragstellers hinzufügen** angeben. Wenn einer der angegebenen Antragstellernamen mit dem Antragsteller des Zertifikats für das SIEM-Systems übereinstimmt, validiert Kaspersky Security Center das Zertifikat dieses SIEM-Systems.

- **Client-Authentifizierung hinzufügen**

Um die Client-Authentifizierung durchzuführen, können Sie entweder Ihr Zertifikat einfügen oder es im Kaspersky Security Center generieren.

- **Zertifikat einfügen**. Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen CA. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

  - **X.509-Zertifikat PEM**. Laden Sie jeweils eine Datei mit Zertifikat über das Feld **Datei mit Zertifikat** und eine Datei mit privatem Schlüssel über das Feld **Datei mit Schlüssel** hoch. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Hochladen der Dateien ist spielt keine Rolle. Wenn beide Dateien hochgeladen sind, geben Sie das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

  - **X.509-Zertifikat PKCS12**. Laden Sie in dem Feld **Datei mit Zertifikat** eine Datei hoch, die ein Zertifikat und dessen privaten Schlüssel enthält. Geben Sie nach dem Hochladen der Datei das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- **Schlüssel generieren**. Sie können in Kaspersky Security Center ein selbstsigniertes Zertifikat generieren. Infolge dessen speichert Kaspersky Security Center das generierte selbstsignierte Zertifikat und Sie können den öffentlichen Teil des Zertifikats oder den SHA1-Fingerabdruck an das SIEM-System übergeben.

- **Datumsformat**

  Je nach den Anforderungen des SIEM-Systems können Sie eines der folgenden Formate auswählen: Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk oder Systemprotokolle.

Wenn Sie das Datenformat für System-Log auswählen, müssen Sie Folgendes angeben:

- **Maximale Größe der Nachricht in Byte**

  Geben Sie die maximale Größe der Nachricht in Byte an, die an das SIEM-System übertragen wird. Jedes Ereignis wird in einer Nachricht übermittelt. Wenn die reale Länge der Nachricht den angegebenen Wert überschreitet, wird die Nachricht abgeschnitten und Daten können verloren gehen. Standardmäßig beträgt die Größe der Nachricht 2048 Bytes. Dieses Feld ist nur verfügbar, falls Sie im Feld **Protokoll** das Format System-Log ausgewählt haben.

5. Wenn Sie möchten, können Sie archivierte Ereignisse aus der Administrationsserver-Datenbank exportieren und das Startdatum angeben, ab dem Sie den Export archivierter Ereignisse starten möchten:

   a. Klicken Sie auf den Link **Geben Sie das Startdatum des Exports an**.

   b. Geben Sie in dem sich öffnenden Abschnitt das Startdatum im Feld **Startdatum des Ereignisexports aus dem System** an.

   c. Klicken Sie auf **OK**.

6. Setzen Sie die Option auf die Position **Auto-Exportieren von Ereignissen in die Datenbank des SIEM-Systems Aktiviert**.

7. Um zu überprüfen, ob die Verbindung mit dem SIEM-System konfiguriert wurde, klicken Sie auf die Schaltfläche **Verbindung prüfen**.

   Die Verbindung mit dem Server des SIEM-Systems wird hergestellt und es wird ein Testereignis gesendet. Der Verbindungsstatus wird angezeigt.

Die Prüfung wird nur für die Protokolle TCP und TLS over TCP durchgeführt.

8. Klicken Sie auf die Schaltfläche **Speichern**.

Der Export in das SIEM-System ist konfiguriert.

Ereignisexport direkt aus der Datenbank

Sie können die Ereignisse direkt aus der Datenbank Kaspersky Security Center extrahieren, ohne die Benutzeroberfläche von Kaspersky Security Center zu verwenden. Die Abfragen können unmittelbar in Bezug auf die öffentlichen Ansichten erstellt und von daraus Daten über die Ereignisse extrahiert werden, oder Sie können eigene Ansichten auf der Grundlage der vorhandenen öffentlichen Ansichten erstellen und die gewünschten Daten von dort beziehen.

Öffentlichen Ansichten

Zur Erhöhung der Benutzerfreundlichkeit sind in der Datenbank von Kaspersky Security Center ein Satz öffentlicher Ansichten vorgesehen. Eine Beschreibung der öffentlichen Ansichten finden Sie im Dokument klakdb.chm.

Die öffentliche Ansicht v_akpub_ev_event enthält einen Satz Felder, die den Einstellungen der Ereignisse in der Datenbank entsprechen. Im Dokument klakdb.chm finden Sie Informationen über die öffentlichen Ansichten, die sich auf andere Objekte von Kaspersky Security Center beziehen, beispielsweise Geräte, Programme, Benutzer. Sie können diese Informationen beim Erstellen von Abfragen verwenden.

In diesem Abschnitt finden Sie Anweisungen zum Ausführen einer SQL-Abfrage mithilfe des Tools "klsql2" sowie eine Beispielabfrage.

Sie können auch beliebige andere Datenbankenanwendungen für das Erstellen der SQL-Abfragen und die Datenbankenansichten verwenden. Informationen zur Anzeige der Verbindungseinstellungen der Datenbank von Kaspersky Security Center, wie z. B. Instanz-Name und Name der Datenbank, finden Sie im entsprechenden Abschnitt.

Eine SQL-Abfrage mit dem Tool "klsql2" ausführen

In diesem Artikel erhalten Sie Anweisungen zum Herunterladen und für die Nutzung des Tools klsql2 sowie zum Ausführen einer SQL-Abfrage mithilfe dieses Tools.

So verwenden Sie das Tool "klsql2":

1. Navigieren Sie zum Tool "klsrvswch" im Installationsordner von Kaspersky Security Center. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center". Verwenden Sie keine Versionen des Tools "klsql2", die für ältere Versionen von Kaspersky Security Center bestimmt sind.

2. Erstellen Sie in einem beliebigen Texteditor eine Datei mit sql-Endung und legen Sie die Datei im selben Ordner wie das Tool ab.

3. Geben Sie den von Ihnen gewünschten SQL-Query in die erstellte sql-Datei ein und speichern Sie die Datei.

4. Geben Sie auf dem Gerät, auf dem der Kaspersky Security Center Administrationsserver installiert ist, in der Befehlszeile den folgenden Befehl für die Ausführung der SQL-Abfrage aus der sql-Datei und zur Speicherung der Ergebnisse in der Datei "result.xml" ein:
   `klsql2 -i src.sql -u <Benutzername> -p <Kennwort> -o result.xml`

   Wobei `<Benutzername>` und `<Kennwort>` den Anmeldeinformationen des Benutzerkontos entsprechen, das Zugriff auf die Datenbank hat.

5. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des Benutzerkontos ein, das Zugriff auf die Datenbank hat.

6. Öffnen Sie die neu erstellten Dateien des Typs "result.xml" und sehen Sie sich die Ergebnisse der SQL-Abfragen an.

Sie können die sql-Datei editieren und darin beliebige SQL-Anfragen an öffentliche Ansichten erstellen. Führen Sie anschließend in der Befehlszeile Ihre SQL-Abfrage aus und speichern Sie das Ergebnis in einer Datei.

Beispiel einer SQL-Abfrage, die mit dem Tool "klsql2" erstellt wurde

Dieser Abschnitt enthält eine beispielhafte SQL-Anfrage, die mittels des Tools "klsql2" ausgeführt wurde.

Die folgenden Beispiele zeigen, wie Sie eine Liste mit den Ereignissen auf den Benutzergeräten für die letzten sieben Tage abrufen und diese nach ihrem Eintrittszeitpunkt sortieren. Die aktuellsten Ereignisse werden zuerst angezeigt.

Beispiel für Microsoft SQL Server:

```
SELECT
  /* ID des Ereignisses */
  e.nId,

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  e.tmRiseTime,

  /* interner Name des Ereignistyps */
  e.strEventType,

  /* angezeigter Name des Ereignisses */
  e.wstrEventTypeDisplayName,

  /* angezeigte Beschreibung des Ereignisses */
  e.wstrDescription,

  /* Name der Gruppe, in der sich das Gerät befindet */
  e.wstrGroupName,

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Beispiel für PostgreSQL:

```
SELECT
  /* ID des Ereignisses */
  "e"."nId",

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  "e"."tmRiseTime",

  /* interner Name des Ereignistyps */
  "e"."strEventType",

  /* angezeigter Name des Ereignisses */
  "e"."wstrEventTypeDisplayName",

  /* angezeigte Beschreibung des Ereignisses */
  "e"."wstrDescription",

  /* angezeigte Beschreibung des Ereignisses */
  "e"."wstrGroupName",

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Beispiel für MySQL oder MariaDB

```
SELECT

  /* ID des Ereignisses */
  `e`.`nId`,

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  `e`.`tmRiseTime`,

  /* interner Name des Ereignistyps */
  `e`.`strEventType`,

  /* angezeigter Name des Ereignisses */
  `e`.`wstrEventTypeDisplayName`,

  /* angezeigte Beschreibung des Ereignisses */
  `e`.`wstrDescription`,

  /* Name der Gerätegruppe */
  `e`.`wstrGroupName`,

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Anzeige des Namens der Datenbank von Kaspersky Security Center

Falls Sie mithilfe von Datenbankverwaltungssystemen für SQL Server, MySQL oder MariaDB auf die Datenbank von Kaspersky Security Center zugreifen möchten, muss der Name der Datenbank bekannt sein, um sie aus dem SQL-Skript-Editor zu verbinden.

Um den Namen der Datenbank von Kaspersky Security Center anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Details der aktuellen Datenbank** aus.

   Der Datenbankname wird im Feld **Name der Datenbank** angegeben. Verwenden Sie diesen Namen der Datenbank für die Verbindung und den Zugriff auf die Datenbank in Ihren SQL-Abfragen.

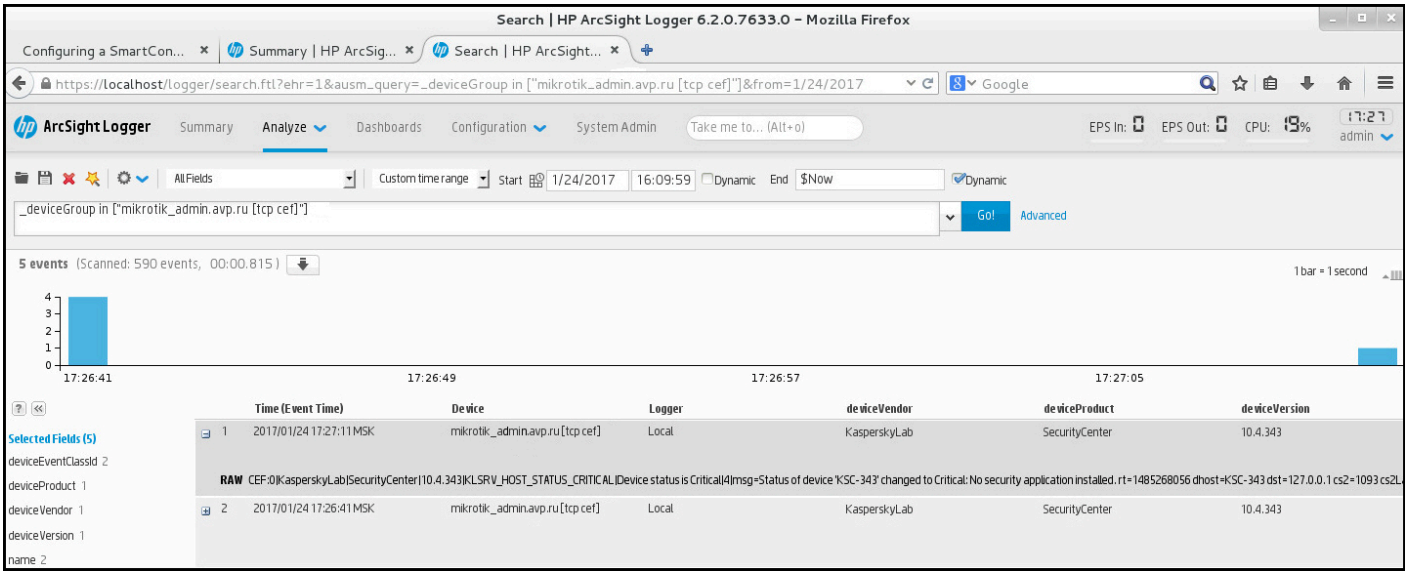
Exportergebnisse anzeigen

Sie können erfahren, ob die Exportprozedur erfolgreich fertig gestellt wurde. Überprüfen Sie dazu, ob das SIEM-System die Nachrichten, in denen die exportierten Ereignisse enthalten sind, erhalten hat.

Wenn die aus Kaspersky Security Center versendeten Ereignisse erhalten und vom SIEM-System richtig interpretiert wurden, bedeutet das, dass die Einstellungen auf beiden Seiten korrekt ausgeführt wurden. Andernfalls prüfen Sie und korrigieren Sie erforderlichenfalls die Einstellungen in Kaspersky Security Center und im SIEM-Systeme.

Nachfolgend finden Sie ein Beispiel für Ereignisse, die ins ArcSight-System exportiert wurden. Das erste Ereignis ist beispielsweise ein kritisches Ereignis des Administrationsservers: "*Gerätestatus ist Kritisch*".

Die Anzeige der exportierten Ereignisse ist vom verwendeten SIEM-System abhängig.



Beispiel für Ereignisse

Arbeiten mit Kaspersky Security Center Web Console in einer Cloud-Umgebung

Dieser Abschnitt bietet Informationen über die Funktionen von Kaspersky Security Center Web Console in Bezug auf die Bereitstellung und Wartung von Kaspersky Security Center in Cloud-Umgebungen wie Amazon Web Services, Microsoft Azure oder Google Cloud.

Um in einer Cloud-Umgebung zu arbeiten, benötigen Sie eine spezielle Lizenz. Wenn Sie keine derartige Lizenz besitzen, werden die Bedienelemente mit Bezug zu Cloud-Geräten nicht angezeigt.

Konfiguration der Cloud-Umgebung in Kaspersky Security Center Web Console

Um Kaspersky Security Center mithilfe des Assistenten zur Konfiguration der Cloud-Umgebung zu konfigurieren, müssen Sie über Folgendes verfügen:

- Spezifische Anmeldeinformationen für eine Cloud-Umgebung:
  - Eine IAM-Rolle, der die Berechtigung zur Abfrage des Cloud-Segments zugewiesen wurde, oder ein IAM-Benutzerkonto, dem die Berechtigung zur Abfrage des Cloud-Segments gewährt wurde (für das Arbeiten mit Amazon Web Services)
  - Eine Azure Anwendungs-ID, ein Kennwort und ein Abonnement (für das Arbeiten mit Microsoft Azure)
  - Eine Google-Client-E-Mail, Projekt-ID und privaten Schlüssel (für das Arbeiten mit Google Cloud)
- Installationspakete:
  - Administrationsagent für Windows
  - Administrationsagent für Linux
  - Kaspersky Endpoint Security für Linux
- Web-Plug-in für Kaspersky Endpoint Security für Linux
- Mindestens eines der folgenden:
  - Installationspaket und Web-Plug-in für Kaspersky Endpoint Security für Windows (empfohlen)
  - Installationspaket und Web-Plug-in für Kaspersky Security für Windows Server

Der Assistent zur Konfiguration der Cloud-Umgebung wird automatisch bei der ersten Verbindung mit dem Administrationsserver über die Verwaltungskonsole gestartet, wenn Sie Kaspersky Security Center aus einem einsatzbereiten Abbild bereitstellen. Sie können den Assistenten auch jederzeit manuell starten.

So starten Sie den Assistenten zur Konfiguration der Cloud-Umgebung manuell:

Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Konfigurieren der Cloud-Umgebung**.

Der Assistent wird gestartet.

Die durchschnittliche Arbeitssitzung zur Konfiguration der Cloud-Umgebung dauert etwa 15 Minuten.

Schritt 1. Überprüfen der erforderlichen Plug-ins und Installationspakete

Dieser Schritt wird nicht angezeigt, wenn Sie bereits über alle unten aufgeführten erforderlichen Web-Plug-Ins und Installationspakete verfügen.

Um eine Cloud-Umgebung zu konfigurieren, benötigen Sie die folgenden Komponenten:

- Installationspakete:
  - Administrationsagent für Windows
  - Administrationsagent für Linux
  - Kaspersky Endpoint Security für Linux
- Web-Plug-in für Kaspersky Endpoint Security für Linux
- Mindestens eines der folgenden:
  - Installationspaket und Web-Plug-in für Kaspersky Endpoint Security für Windows (empfohlen)
  - Installationspaket und Web-Plug-in für Kaspersky Security für Windows Server

    Wir empfehlen Ihnen, Kaspersky Endpoint Security für Windows anstelle von Kaspersky Security für Windows Server zu verwenden.

Kaspersky Security Center erkennt automatisch die Komponenten, über die Sie bereits verfügen, und listet nur die fehlenden auf. Laden Sie die aufgelisteten Komponenten herunter, indem Sie auf die Schaltfläche **Anwendungen zum Herunterladen auswählen** klicken und anschließend die erforderlichen Plug-Ins und Installationspakete auswählen. Nachdem Sie eine Komponente heruntergeladen haben, können Sie die Schaltfläche **Aktualisieren** verwenden, um die Liste der fehlenden Komponenten zu aktualisieren.

Schritt 2. Lizenzieren des Programms

Dieser Schritt wird nur angezeigt, wenn Sie BYOL AMI verwenden und die Anwendung nicht mit einer Lizenz für Kaspersky Security for Virtualization oder für Kaspersky Hybrid Cloud Security aktiviert haben.

Geben Sie den Lizenzschlüssel an und klicken Sie auf **Weiter**, um fortzufahren.

Der Lizenzschlüssel wird zur Datenverwaltung des Administrationsservers hinzugefügt.

Wenn Sie den Assistenten erneut ausführen, wird dieser Schritt nicht angezeigt.

Schritt 3. Auswählen der Cloud-Umgebung und Autorisierung

Dieser Abschnitt beschreibt Funktionen, die nur auf Kaspersky Security Center 12.1 oder einer aktuelleren Version angewendet werden können.

Geben Sie die folgenden Einstellungen an:

- **Cloud-Umgebung**

  Wählen Sie die Cloud-Umgebung aus, in der Sie Kaspersky Security Center AWS, Azure oder Google Cloud verteilen.

  Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, wählen Sie zunächst eine Umgebung aus und führen Sie anschließend den Assistenten erneut aus.

- **Verbindungsname**

  Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

  Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

  Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

Geben Sie Ihre Anmeldedaten ein, um eine Autorisierung für die Cloud-Umgebung zu erhalten, die Sie ausgewählt haben.

AWS

Wenn Sie AWS als Cloud-Segments-Typ ausgewählt haben, benötigen Sie eine IAM-Rolle oder einen AWS IAM-Zugriffsschlüssel, um das Cloud-Segment weiter abzufragen.

- **AWS IAM-Rolle, die einer EC2-Instance zugewiesen ist**

  Wählen Sie diese Option aus, wenn Sie eine IAM-Rolle mit den erforderlichen Rechten für den Administrationsserver haben.

- **AWS IAM-Benutzer**

  Wählen Sie diese Option aus, wenn Sie über einen AWS IAM-Zugriffsschlüssel verfügen. Geben Sie Ihre Schlüsseldaten ein:

  - **Zugriffsschlüssel-ID**

    ID des IAM-Zugriffsschlüssels (eine Abfolge von alphanumerischen Zeichen). Sie haben die Schlüssel-ID bei der Erstellung des IAM-Benutzerkontos erhalten.

    Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

- **Geheimer Schlüssel**

  Geheimer Schlüssel, den Sie gemeinsam mit der ID des Zugriffsschlüssels erhalten haben, als Sie das IAM-Benutzerkonto erstellt haben.

  Die Zeichen des geheimen Schlüssels werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des geheimen Schlüssels begonnen haben, wird die Schaltfläche **Anzeigen** angezeigt. Klicken Sie auf diese Schaltfläche und halten Sie diese so lange wie nötig gedrückt, um die eingegebenen Zeichen anzuzeigen.

  Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

  Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

Azure

Wenn Sie Azure als Cloud-Segment-Typ ausgewählt haben, passen Sie die folgenden Verbindungseinstellungen an, die im Weiteren für die Abfrage des Cloud-Segments verwendet werden:

- **Anwendungs-ID für Azure**

  Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

  Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

- **Azure-Abonnement-ID**

  Sie haben das Abonnement auf dem Azure-Portal erstellt.

- **Azure-App-Kennwort**

  Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

  Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

  Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

- **Name des Azure-Speicherkontos**

  Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

- **Zugriffsschlüssel für Azure-Speicher**

  Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Security Center erstellt haben.

  Sie finden den Schlüssel im Abschnitt "Übersicht über das Azure-Speicherkonto" im Unterabschnitt "Schlüssel".

  Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

Google Cloud

Wenn Sie Google Cloud als Cloud-Segment-Typ ausgewählt haben, passen Sie die folgenden Verbindungseinstellungen an, die im Weiteren für die Abfrage des Cloud-Segments verwendet werden:

- **E-Mail-Adresse des Clients**

  Client-E-Mail ist die E-Mail-Adresse, die Sie für Ihr Projekt bei Google Cloud registriert haben.

- **Projekt-ID**

  Projekt-ID ist die ID, die Sie erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben.

- **Privater Schlüssel**

  Privater Schlüssel ist die Zeichenfolge, die Sie als privaten Schlüssel erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben. Um Fehler zu vermeiden können Sie die Zeichenfolge kopieren und einfügen.

  Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

Die von Ihnen angegebene Verbindung wird in den Programmeinstellungen gespeichert.

In dem Assistenten zur Konfiguration der Cloud-Umgebung kann nur ein Segment angegeben werden. Sie können später weitere Verbindungen für die Verwaltung anderer Cloud-Segmente angeben.

Klicken Sie auf **Weiter** um fortfahren.

Schritt 4. Abfragen des Segments, Konfigurieren der Cloud-Synchronisation und Wählen weiterer Maßnahmen

In diesem Schritt wird die Abfrage von Cloud-Segmenten gestartet und eine spezielle Administrationsgruppe für Cloud-Geräte wird automatisch erstellt. Die bei der Abfrage gefundene Geräte werden in dieser Gruppe platziert. Der Zeitplan für die Abfrage des Cloud-Segments ist konfiguriert (standardmäßig alle 5 Minuten, Sie können diese Einstellung später ändern).

Des Weiteren wird eine Regel für das automatische Verschieben **Synchronisierung mit Cloud** erstellt. Bei jedem nachfolgenden Scannen des Cloud-Netzwerks werden die gefundenen virtuellen Geräte in die entsprechende Untergruppe innerhalb der Gruppe **Verwaltete Geräte\Cloud** verschoben.

Passen Sie die folgenden Einstellungen an:

- **Administrationsgruppen mit Cloud-Struktur synchronisieren**

  Wenn diese Option aktiviert ist, wird innerhalb der Gruppe **Verwaltete Geräte** automatisch die Gruppe **Cloud** erstellt und eine Gerätesuche in der Cloud ausgeführt. Die Instances und virtuellen Maschinen, die jeweils während der Untersuchung des Cloud-Netzwerks gefunden werden, werden in die Cloud-Gruppe verschoben. Die Struktur der Verwaltungsuntergruppen innerhalb dieser Gruppe stimmt mit der Struktur Ihres Cloud-Segments überein (in AWS werden Verfügbarkeitszone und Zuordnungsgruppen nicht in der Struktur dargestellt; in Azure werden Subnetze nicht in der Struktur dargestellt). Geräte, die nicht als Instances in der Cloud-Umgebung identifiziert werden, befinden sich in der Gruppe **Nicht zugeordnete Geräte**. Eine solche Gruppenstruktur ermöglicht, mithilfe der Aufgaben zur Gruppeninstallation Antiviren-Programme auf Instances zu installieren und verschiedene Richtlinien für verschiedene Gruppen anzupassen.

Wenn diese Option deaktiviert ist, wird auch die Gruppe **Cloud** erstellt und eine Gerätesuche in der Cloud wird gestartet; Untergruppen, die der Struktur des Cloud-Segments entsprechen, werden jedoch innerhalb der Gruppe nicht erstellt. Alle gefundenen Instances befinden sich in der **Cloud**-Administrationsgruppe und werden daher als einheitliche Liste angezeigt. Wenn während der Ausführung von Kaspersky Security Center eine Synchronisierung vorgenommen werden muss, können Sie die Eigenschaften der Regel **Synchronisierung mit Cloud** ändern und diese erzwingen. Durch das Erzwingen der Regel wird die Struktur der Gruppen innerhalb der Cloud-Gruppe neu angeordnet, sodass sie der Struktur Ihres Cloud-Segments entspricht.

Diese Option ist standardmäßig deaktiviert.

- **Schutz bereitstellen**

  Wenn diese Option ausgewählt ist, erstellt der Assistent eine Aufgabe zur Installation der Sicherheitsanwendungen auf den Instances. Nach dem Fertigstellen des Assistenten wird automatisch der Assistent für die Bereitstellung des Schutzes auf den Geräten in Ihren Cloud-Segmenten gestartet, und Sie können auf diesen Geräten den Administrationsagenten und die Sicherheitsanwendungen installieren.

  Kaspersky Security Center kann die Bereitstellung mit seinen nativen Instrumenten durchführen. Wenn Sie keine Berechtigung haben, um die Anwendungen auf den EC2-Instances oder auf virtuellen Azure-Maschinen zu installieren, können Sie die Aufgabe **Remote-Installation** manuell konfigurieren und ein Benutzerkonto mit den erforderlichen Berechtigungen angeben. In diesem Fall kann die Aufgabe "Remote-Installation" nicht für Geräte verwendet werden, die mit AWS API oder Azure gefunden wurden. Diese Aufgabe kann nur für Geräte verwendet werden, die mittels Abfrage des Active Directory, Abfrage der Windows-Domänen oder Durchsuchen der IP-Bereiche gefunden wurden.

  Wenn diese Option nicht ausgewählt ist, wird der Assistent für die Bereitstellung des Schutzes nicht gestartet und auch die Aufgaben zur Installation der Sicherheitsanwendungen auf Instances nicht erstellt. Sie können beide Aktionen später manuell durchführen.

Wenn Sie die Option Schutz bereitstellen auswählen, wird der Abschnitt **Geräte neu starten** sichtbar. In diesem Abschnitt müssen Sie Aktionen für den Fall festlegen, dass ein Zielgerät neu gestartet werden soll. Bestimmen Sie, ob Instances erneut geladen werden sollen, wenn im Verlauf der Programminstallation ein Neustart des Geräte-Betriebssystems erforderlich ist:

- **Nicht neu starten**

  Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung nicht neu gestartet.

- **Neu starten**

  Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung neu gestartet.

Klicken Sie auf **Weiter** um fortfahren.

Für Google Cloud können Sie die Bereitstellung ausschließlich mit den nativen Werkzeugen von Kaspersky Security Center durchführen. Wenn Sie Google Cloud ausgewählt haben, ist die Option **Schutz bereitstellen** nicht verfügbar.

Schritt 5. Auswählen der Anwendung, für die eine Richtlinie und Aufgaben erstellt werden sollen

Dieser Schritt wird nur angezeigt, wenn Sie über Installationspakete und Plug-ins sowohl für Kaspersky Endpoint Security für Windows als auch für Kaspersky Security für Windows Server verfügen. Wenn Sie nur für eines dieser Programme über ein Plug-in und ein Installationspaket verfügen, wird dieser Schritt übersprungen und die Kaspersky Security Center erstellt eine Richtlinie und Aufgaben für das vorhandene Programm.

Wählen Sie ein Programm aus, für das Sie eine Richtlinie und Aufgaben erstellen möchten:

- Kaspersky Endpoint Security für Windows
- Kaspersky Security für Windows Server

Schritt 6. Konfiguration von Kaspersky Security Network für Kaspersky Security Center

Legen Sie die Einstellungen für das Übertragen von Informationen über die Ausführung von Kaspersky Security Center in die Wissensdatenbank von Kaspersky Security Network (KSN) fest. Wählen Sie eine der folgenden Varianten aus:

- **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network**

  Kaspersky Security Center und die verwalteten Programme, die auf Client-Geräten installiert sind, übertragen ihre Vorgangsdetails automatisch an Kaspersky Security Network. Die Zusammenarbeit mit Kaspersky Security Network gewährleistet ein schnelleres Datenbanken-Update mit Daten über Viren und Bedrohungen, wodurch die Reaktionsgeschwindigkeit auf neue Sicherheitsgefährdungen erhöht wird.

- **Ich lehne die Nutzungsbedingungen von Kaspersky Security Network ab**

  Kaspersky Security Center und verwaltete Programme senden keine Informationen an Kaspersky Security Network.

  Wenn Sie diese Option auswählen, wird die Verwendung von Kaspersky Security Network deaktiviert.

Kaspersky empfiehlt die Teilnahme an Kaspersky Security Network.

Die KSN-Erklärungen verwalteter Programme können ebenfalls angezeigt werden. Wenn Sie die Nutzungsbedingungen von Kaspersky Security Network akzeptieren, überträgt das verwaltete Programm Daten an Kaspersky. Wenn Sie der Teilnahme an Kaspersky Security Network nicht zustimmen, überträgt das verwaltete Programm keine Daten an Kaspersky (Sie können diese Einstellung später in der Programmrichtlinie ändern).

Klicken Sie auf **Weiter** um fortfahren.

Schritt 7. Erstellen einer Erstkonfiguration des Schutzes

Sie können die Liste mit Richtlinien und Aufgaben, die erstellt werden, überprüfen.

Warten Sie, bis die Erstellung der Richtlinien und Aufgaben abgeschlossen ist, und klicken Sie auf **Weiter**, um fortzufahren. Klicken Sie auf der Letzten Seite des Assistenten auf **Fertigstellen**, um ihn zu verlassen.

Abfrage von Netzwerksegmenten mittels Kaspersky Security Center Web Console

Der Administrationsserver erhält Daten über die Netzwerkstruktur (und der darin befindlichen Geräte) anhand von regelmäßigen Abfragen der Cloud-Segmente durch die Tools der AWS-API, Azure-API oder Google-API. Auf Grundlage der empfangenen Daten aktualisiert Kaspersky Security Center den Inhalt der Ordner "Nicht zugeordnete Geräte" und "Verwaltete Geräte". Wenn Sie das automatische Verschieben von Geräten in Administrationsgruppen eingerichtet haben, werden die im Netzwerk gefundenen Geräte in Administrationsgruppen aufgenommen.

Zur Abfrage von Cloud-Segmenten durch den Administrationsserver sind entsprechende Rechte erforderlich, die mit einer IAM-Rolle, einem IAM-Benutzerkonto (in AWS), einer Anwendungs-ID und einem Kennwort (in Azure) oder mit einer Google-Client-E-Mail, Google-Projekt-ID und privaten Schlüssel (in Google Cloud) gewährt werden.

Sie können Verbindungen, hinzufügen und entfernen sowie für jedes Cloud-Segment einen Zeitplan für die Abfrage einrichten.

Hinzufügen von Verbindungen für die Abfrage von Cloud-Segmenten

Um die Verbindung für die Abfrage von Cloud-Segmenten zur Liste der verfügbaren Verbindungen hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → Cloud**.
2. Klicken Sie im folgenden Fenster auf **Eigenschaften**.
3. Klicken Sie im folgenden Fenster **Einstellungen** auf **Hinzufügen**.

   Das Fenster **Einstellungen des Cloud-Segments** wird geöffnet.
4. Geben Sie den Namen der Cloud-Umgebung für die Verbindung an, die im Weiteren für die Abfrage des Cloud-Segments verwendet werden:

   - **Cloud-Umgebung**

     Wählen Sie die Cloud-Umgebung aus, in der Sie Kaspersky Security Center AWS, Azure oder Google Cloud verteilen.

     Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, wählen Sie zunächst eine Umgebung aus und führen Sie anschließend den Assistenten erneut aus.

   - **Verbindungsname**

     Geben Sie einen Namen für die Verbindung ein. Der Name darf nicht mehr als 256 Zeichen enthalten. Es sind nur UNICODE-Zeichen zulässig.

     Dieser Name wird auch als Name der Administrationsgruppe für die Cloud-Geräte verwendet.

     Wenn Sie mit mehr als einer Cloud-Umgebung arbeiten möchten, ist es empfehlenswert, die Namen der Umgebungen in die Verbindungsnamen aufzunehmen, beispielsweise "Azure-Segment," "AWS-Segment" oder "Google-Segment".

5. Geben Sie Ihre Anmeldedaten ein, um eine Autorisierung für die Cloud-Umgebung zu erhalten, die Sie ausgewählt haben.

   - Wenn Sie AWS ausgewählt haben, geben Sie die folgenden Einstellungen an:

     - **AWS IAM-Rolle verwenden**

       Wählen Sie diese Option aus, wenn Sie bereits eine IAM-Rolle für den Administrationsserver zur Verwendung mit AWS-Diensten erstellt haben.

     - **Anmeldedaten des AWS IAM-Benutzerkontos**

       Wählen Sie diese Variante aus, wenn Sie ein IAM-Benutzerkonto mit den erforderlichen Rechten besitzen und die ID des Schlüssels und den geheimen Schlüssel eingeben können.

       Wenn Sie "Anmeldedaten des AWS IAM-Benutzerkontos " angegeben haben, geben Sie die folgenden Daten ein:

       - **Zugriffsschlüssel-ID**

         ID des IAM-Zugriffsschlüssels (eine Abfolge von alphanumerischen Zeichen). Sie haben die Schlüssel-ID bei der Erstellung des IAM-Benutzerkontos erhalten.

         Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

       - **Geheimer Schlüssel**

         Geheimer Schlüssel, den Sie gemeinsam mit der ID des Zugriffsschlüssels erhalten haben, als Sie das IAM-Benutzerkonto erstellt haben.

         Die Zeichen des geheimen Schlüssels werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des geheimen Schlüssels begonnen haben, wird die Schaltfläche **Anzeigen** angezeigt. Klicken Sie auf diese Schaltfläche und halten Sie diese so lange wie nötig gedrückt, um die eingegebenen Zeichen anzuzeigen.

         Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

       Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

   - Wenn Sie Azure ausgewählt haben, geben Sie die folgenden Einstellungen an:

     - **Anwendungs-ID für Azure**

       Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

       Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

     - **Azure-Abonnement-ID**

       Sie haben das Abonnement auf dem Azure-Portal erstellt.

     - **Azure-App-Kennwort**

       Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

- **Name des Azure-Speicherkontos**

  Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

- **Zugriffsschlüssel für Azure-Speicher**

  Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Security Center erstellt haben.

  Sie finden den Schlüssel im Abschnitt "Übersicht über das Azure-Speicherkonto" im Unterabschnitt "Schlüssel".

  Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

Wenn Sie Google Cloud ausgewählt haben, geben Sie die folgenden Einstellungen an:

- **E-Mail-Adresse des Clients**

  Client-E-Mail ist die E-Mail-Adresse, die Sie für Ihr Projekt bei Google Cloud registriert haben.

- **Projekt-ID**

  Projekt-ID ist die ID, die Sie erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben.

- **Privater Schlüssel**

  Privater Schlüssel ist die Zeichenfolge, die Sie als privaten Schlüssel erhalten haben, als Sie Ihr Projekt bei Google Cloud registriert haben. Um Fehler zu vermeiden können Sie die Zeichenfolge kopieren und einfügen.

  Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

6. Klicken Sie bei Bedarf auf **Abfragezeitplan festlegen** und passen Sie die Standardeinstellungen an.

Die Verbindung wird in den Programmeinstellungen gespeichert.

Nach der ersten Abfrage des neuen Cloud-Segments erscheint in der Administrationsgruppe **Verwaltete Geräte\Cloud** eine Untergruppe, die diesem Segment entspricht.

Wenn die von Ihnen angegebenen Benutzerdaten falsch sind, werden bei der Abfrage des Cloud-Segments keine Instances gefunden und in der Administrationsgruppe **Verwaltete Geräte\Cloud** wird keine neue Untergruppe angezeigt.

Entfernen einer Verbindung für die Abfrage von Cloud-Segmenten

Wenn Sie ein bestimmtes Cloud-Segment nicht mehr abfragen müssen, können Sie die ihm entsprechende Verbindung aus der Liste der verfügbaren Verbindungen löschen. Sie können die Verbindung auch löschen, wenn z. B. die Berechtigung zur Abfrage des Cloud-Segments an einen anderen Benutzer mit anderen Anmeldedaten übertragen wurde.

Gehen Sie folgendermaßen vor, um eine Verbindung zu löschen:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → Cloud**.
2. Klicken Sie im folgenden Fenster auf **Eigenschaften**.
3. Klicken Sie im folgenden Fenster **Einstellungen** auf den Namen des Segments, dass Sie löschen möchten.
4. Klicken Sie auf die Schaltfläche **Löschen**.
5. Klicken Sie im folgenden Fenster auf die Schaltfläche **OK**, um die Auswahl zu bestätigen.

Die Verbindung wurde gelöscht. Die Geräte in dem der Verbindung entsprechenden Cloud-Segment werden automatisch aus den Administrationsgruppen entfernt.

Konfiguration des Abfragezeitplans durch Kaspersky Security Center Web Console anpassen

Die Abfrage des Cloud-Segments erfolgt nach Zeitplan. Sie können das Intervall festlegen, in dem die Abfrage durchgeführt wird.

Das Intervall für die Abfrage wird in den Einstellungen zur Konfiguration der Cloud-Umgebung automatisch auf 5 Minuten festgelegt. Sie können diesen Wert jederzeit ändern und einen anderen Zeitplan festlegen. Es wird jedoch nicht empfohlen, die Einstellungen der Abfrage so anzupassen, dass sie öfter als alle 5 Minuten durchgeführt wird, da dies zu Fehlern in der Ausführung der API führen kann.

Gehen Sie folgendermaßen vor, um den Abfragezeitplan für das Cloud-Segment anzupassen:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → Cloud**.
2. Klicken Sie im folgenden Fenster auf **Eigenschaften**.
3. Klicken Sie im folgenden Fenster **Einstellungen** auf Namen des Segments, für das Sie einen Abfragezeitplan konfigurieren möchten.

   Das Fenster **Einstellungen des Cloud-Segments** wird geöffnet.
4. Klicken Sie im Fenster **Einstellungen des Cloud-Segments** auf **Abfragezeitplan festlegen**.

   Das Fenster **Zeitplan** wird geöffnet.
5. Geben Sie in dem Fenster **Zeitplan** die folgenden Einstellungen an:

   - **Start nach Zeitplan**

Varianten für den Zeitplan der Abfrage:

- **Alle n Tage**

  Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

  Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- Alle n Minuten

  Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

  Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

- Nach Wochentagen

  Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

  Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- Monatlich, an angegebenen Tagen der gewählten Wochen

  Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

- **Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.Startintervall (Min.)**

  Geben Sie an, wofür n steht (Minuten oder Tage).

- **Beginnend ab**

  Geben Sie an, wann mit der ersten Abfrage begonnen werden soll.

- **Übersprungene Aufgaben starten**

  Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

  Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

  Diese Option ist standardmäßig aktiviert.

6. Speichern Sie die Änderungen.

Der Abfragezeitplan für das Segment wurde konfiguriert und gespeichert.

Anzeigen der Ergebnisse der Abfrage des Cloud-Segments durch Kaspersky Security Center Web Console

Sie können die Ergebnisse der Abfrage des Cloud-Segments, d. h. die Liste der vom Administrationsserver verwalteten Cloud-Geräte, anzeigen.

Um die Ergebnisse der Abfrage des Cloud-Segments anzuzeigen, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → Cloud**.

Dies zeigt die zur Abfrage verfügbaren Cloud-Segmente an.

Anzeigen der Eigenschaften von Cloud-Geräten durch Kaspersky Security Center Web Console

Sie können die Eigenschaften jedes Cloud-Geräts anzeigen.

Um die Eigenschaften eines Cloud-Gerätes anzuzeigen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte) → Verwaltete Geräte**.
2. Klicken Sie auf den Namen des Geräts, dessen Eigenschaften Sie anzeigen möchten.
   Es wird Eigenschaftenfenster geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.
3. Wenn Sie speziell die Eigenschaften für Cloud-Geräte anzeigen wollen, wählen Sie im Eigenschaftenfenster den Abschnitt **System** aus.
   Die angezeigten Eigenschaften sind abhängig von der Cloud-Plattform des Geräts.
   Für Geräte in AWS werden die folgenden Eigenschaften angezeigt:
   - **Gefunden mithilfe von API** (Wert: **AWS**)
   - **Cloud-Region**
   - **Cloud-VPC**
   - **Cloud Availability Zone (Verfügbarkeitszone)**
   - **Cloud-Subnetz**
   - **Cloud-Placement-Gruppe** (Dieses Element wird nur angezeigt, wenn die Instance zu einer Platzierungsgruppe gehört - andernfalls wird es nicht angezeigt)

   Für Geräte in Azure werden die folgenden Eigenschaften angezeigt:
   - **Gefunden mithilfe von API** (Wert: **Microsoft Azure**)
   - **Cloud-Region**
   - **Cloud-Subnetz**

   Für Geräte in Google Cloud werden die folgenden Eigenschaften angezeigt:
   - **Gefunden mithilfe von API** (Wert: **Google Cloud**)
   - **Cloud-Region**
   - **Cloud-VPC**

- **Cloud Availability Zone (Verfügbarkeitszone)**
- **Cloud-Subnetz**

Synchronisation mit der Cloud: Konfigurieren der Verschiebungsregel

Im Rahmen der Ausführung der Umgebung zur Cloud-Konfiguration wird die Regel zur Synchronisierung mit Cloud automatisch erstellt. Die Regel ermöglicht das automatische Verschieben von Geräten, die bei den einzelnen Abfragen gefunden werden, aus der Gruppe "Nicht zugeordnete Geräte" in die Gruppe "Verwaltete Geräte\Cloud", um diese Geräte für die zentralisierte Verwaltung verfügbar zu machen. Standardmäßig wird die Regel nach der Erstellung aktiviert. Sie können die Regel jederzeit deaktivieren, ändern oder erzwingen.

Um die Eigenschaften der Regel Synchronisierung mit Cloud zu ändern bzw. zu erzwingen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Verschiebungsregeln**.

   Dies öffnet eine Liste mit Verschiebungsregeln.

2. Wählen Sie in der Liste mit Verschiebungsregeln **Mit der Cloud synchronisieren** aus.

   Daraufhin wird das Eigenschaftenfenster der Regel geöffnet.

3. Geben Sie erforderlichenfalls die folgenden Einstellungen auf der Registerkarte **Regelbedingungen** im Abschnitt **Cloud-Segmente** an:

   - **Gerät befindet sich in einem Cloud-Segment**

     Die Regel wird nur auf Geräte verteilt, die sich im ausgewählten Cloud-Segment befinden. Andernfalls wird die Regel auf alle gefundenen Geräte angewendet.

     Diese Variante ist standardmäßig ausgewählt.

   - **Untergeordnete Objekte einschließen**

     Die Regel wird auf alle Geräten im ausgewählten Segment und in allen untergeordneten Cloud-Abschnitten verteilt. Anderenfalls wird die Regel nur auf Geräte verteilt, die sich im Stammsegment befinden.

     Diese Variante ist standardmäßig ausgewählt.

   - **Geräte aus untergeordneten Objekten in entsprechende Gruppen verschieben**

     Wenn diese Option aktiviert ist, werden Geräte aus untergeordneten Objekten automatisch in die Untergruppen verschoben, die ihrer Struktur entsprechen.

     Wenn diese Option deaktiviert ist, werden Geräte aus untergeordneten Objekten automatisch ohne weitere Aufteilung in den Stamm der Cloud-Untergruppe verschoben.

     Diese Option ist standardmäßig aktiviert.

   - **Untergruppen erstellen, die Containern von neu erkannten Geräten entsprechen**

     Wenn diese Option aktiviert ist und in der Struktur der Gruppe **Verwaltete Geräte\Cloud** keine Untergruppen vorhanden sind, die jenem Abschnitt entsprechen würden, in dem sich das Gerät befindet, werden die entsprechenden Untergruppen von Kaspersky Security Center erstellt. Wird zum Beispiel ein neues Subnetz während der Gerätesuche gefunden, wird eine neue Gruppe mit dem gleichen Namen in der Gruppe **Verwaltete Geräte\Cloud** erstellt.

Wenn diese Option deaktiviert ist, erstellt Kaspersky Security Center keine neuen Untergruppen. Wenn zum Beispiel ein neues Subnetz während der Netzwerkabfrage gefunden wird, wird eine neue Gruppe mit dem gleichen Namen in der Gruppe **Verwaltete Geräte\Cloud** erstellt und die im Subnetz enthaltenen Geräte werden in die Gruppe **Verwaltete Geräte\Cloud** verschoben.

Diese Option ist standardmäßig aktiviert.

- **Untergruppen ohne Entsprechungen in Cloud-Segmenten löschen**

  Wenn diese Option aktiviert ist, löscht das Programm alle Untergruppen, die keinen der existierenden Cloud-Objekten entsprechen, aus der Cloud-Gruppe.

  Wenn diese Option deaktiviert ist, werden Untergruppen, die keinem der existierenden Cloud-Objekten entsprechen, beibehalten.

  Diese Option ist standardmäßig aktiviert.

Wenn Sie bei der Konfiguration der Cloud-Umgebung die Option **Administrationsgruppen mit Cloud-Struktur synchronisieren** aktiviert haben, wird die Regel **Mit der Cloud synchronisieren** mit den aktivierten Optionen **Untergruppen erstellen, die Containern von neu erkannten Geräten entsprechen** und **Untergruppen ohne Entsprechungen in Cloud-Segmenten löschen** erstellt.

Wenn Sie die Option **Administrationsgruppen mit Cloud-Struktur synchronisieren** nicht aktiviert haben, wird die Regel **Mit der Cloud synchronisieren** mit diesen Optionen deaktiviert erstellt. Wenn Ihre Arbeit mir Kaspersky Security Center erfordert, dass die Struktur der untergeordneten Gruppen in der Untergruppe **Verwaltete Geräte\Cloud** der Struktur des Cloud-Segments entspricht, aktivieren Sie die Optionen **Untergruppen erstellen, die Containern von neu erkannten Geräten entsprechen** und **Untergruppen ohne Entsprechungen in Cloud-Segmenten löschen** in den Einstellungen der Regel und erzwingen Sie anschließend die Regel.

4. Wählen Sie in der Dropdown-Liste **Gerät mittels API erkannt** einen Wert aus:

   - **Nein** Das Gerät wird nicht mithilfe von AWS-, Azure- oder Google-API gefunden, das heißt, es befindet sich entweder außerhalb der Cloud-Umgebung oder es befindet sich zwar in der Cloud-Umgebung, ist aber aus irgendwelchen Gründen nicht für die Suche mithilfe des API verfügbar.
   - **AWS**. Das Gerät wird mithilfe von AWS API gefunden, d. h. es befindet sich definitiv in der AWS Cloud-Umgebung.
   - **Azure**. Das Gerät wird mithilfe von Azure API gefunden, d. h. es befindet sich definitiv in der Azure Cloud-Umgebung.
   - **Google Cloud**. Das Gerät wird mithilfe von Google API gefunden, d. h. es befindet sich definitiv in der Google Cloud-Umgebung.
   - Kein Wert. Es wird kein Kriterium angewandt.

5. Bei Bedarf können Sie weitere Eigenschaften der Regel in den anderen Abschnitten anpassen.

Die Verschiebungsregel wird konfiguriert.

Remote-Installation von Programmen auf virtuellen Maschinen von Azure

Für die Installation von Programmen auf den virtuellen Maschinen von Microsoft Azure benötigen Sie eine gültige Lizenz.

Kaspersky Security Center unterstützt die folgenden Szenarien:

- Ein Client-Gerät wird mittels der Azure-API gefunden; die Installation erfolgt ebenfalls mittels einer API. Wenn Sie die Azure-API verwenden, können Sie nur die folgenden Programme installieren:
  - Kaspersky Endpoint Security für Linux
  - Kaspersky Endpoint Security für Windows
  - Kaspersky Security für Windows Server
- Ein Client-Gerät wird mittels der Azure-API gefunden; die Installation wird unter Verwendung von Verteilungspunkten durchgeführt oder – wenn dieser nicht zur Verfügung steht – manuell mittels Standalone-Installationspaketen. Mit dieser Methode können Sie alle Programme installieren, die von Kaspersky Security Center unterstützt werden.

So erstellen Sie eine Aufgabe zur Remote-Installation eines Programms auf virtuellen Maschinen von Azure:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Folgen Sie den Anweisungen des Assistenten:
   a. Wählen Sie den Aufgabentyp **Remote-Installation eines Programms** aus.
   b. Wählen Sie auf der Seite **Installationspakete** die Option **Remote-Installation mittels API von Microsoft Azure**.
   c. Geben Sie bei der Auswahl des Kontos für den Zugriff auf Geräte ein vorhandenes Azure-Konto an oder klicken Sie auf **Hinzufügen** und geben Sie die Anmeldeinformationen Ihres Azure-Kontos ein:
      - **Azure-Kontoname**

        Geben Sie einen beliebigen Namen für die von Ihnen angegebenen Anmeldeinformationen ein. Dieser Name wird in der Liste der Benutzerkonten zur Ausführung der Aufgabe angezeigt.
      - **Anwendungs-ID für Azure**

        Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

        Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.
      - **Azure-App-Kennwort**

        Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

        Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.
   d. Wählen Sie die notwendigen Geräte aus der Gruppe **Verwaltete Geräte\Cloud** aus.

Nachdem der Assistent abgeschlossen ist, wird die Aufgabe zur Remote-Installation des Programms in der Aufgabenliste angezeigt.

Erstellen der Aufgabe zum Backup der Daten des Administrationsservers unter Verwendung eines Cloud-DBMS

Backup-Aufgaben sind Aufgaben des Administrationsservers. Sie erstellen eine Backup-Aufgabe, wenn Sie ein in einer Cloud-Umgebung befindliches DBMS verwenden möchten (AWS oder Azure).

Um eine Aufgabe zum Anlegen eines Backups des Administrationsservers zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie auf der ersten Seite des Assistenten in der Liste **Programm** die Option **Kaspersky Security Center 15.1** und in der Liste **Aufgabentyp** die Option **Backup der Daten des Administrationsservers anlegen** aus.
4. Geben Sie auf der entsprechenden Seite des Assistenten die folgenden Informationen an:

   - Wenn Sie mit einer Datenbank in AWS arbeiten:

     - **Name des S3-Buckets**

       Name des S3-Buckets, den Sie für das Backup erstellt haben.

     - **ID des Zugriffsschlüssels**

       Sie haben die Schlüssel-ID (Abfolge von alphanumerischen Zeichen) erhalten, als Sie das IAM-Benutzerkonto erstellt haben, um mit der Speicher-Instanz des S3-Buckets zu arbeiten.

       Dieses Feld ist verfügbar, wenn Sie RDS-Datenbank auf einem S3-Bucket ausgewählt haben.

     - **Geheimer Schlüssel**

       Geheimer Schlüssel, den Sie gemeinsam mit der ID des Zugriffsschlüssels erhalten haben, als Sie das IAM-Benutzerkonto erstellt haben.

       Die Zeichen des geheimen Schlüssels werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des geheimen Schlüssels begonnen haben, wird die Schaltfläche **Anzeigen** angezeigt. Klicken Sie auf diese Schaltfläche und halten Sie diese so lange wie nötig gedrückt, um die eingegebenen Zeichen anzuzeigen.

       Dieses Feld ist verfügbar, wenn Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel und nicht die IAM-Rolle ausgewählt haben.

   - Wenn Sie mit einer Datenbank in Microsoft Azure arbeiten:

     - **Name des Azure-Speicherkontos**

       Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center zu arbeiten.

     - **Azure-Abonnement-ID**

       Sie haben das Abonnement auf dem Azure-Portal erstellt.

- **Azure-Kennwort**

  Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

  Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

- **Anwendungs-ID für Azure**

  Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

  Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

- **Name des Azure SQL-Servers**

  Der Name und die Gruppe der Ressourcen sind in den Eigenschaften Ihres Azure SQL-Servers verfügbar.

- **Azure SQL-Serverressourcengruppe**

  Der Name und die Gruppe der Ressourcen sind in den Eigenschaften Ihres Azure SQL-Servers verfügbar.

- **Zugriffsschlüssel für Azure-Speicher**

  Verfügbar in den Eigenschaften Ihres Speicherkontos im Abschnitt "Zugriffsschlüssel". Sie können einen der Schlüssel (Schlüssel1 oder Schlüssel2) verwenden.

Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt. Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die Standardeinstellungen der Aufgabe direkt nach der Erstellung der Aufgabe anpassen. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

Ferndiagnose der Client-Geräte

Sie können die Ferndiagnose für das Remote-Ausführen der folgenden Vorgänge auf Windows- und Linux-basierten Client-Geräten verwenden:

- Ablaufverfolgung aktivieren und deaktivieren, Ablaufverfolgungsstufe ändern und Ablaufverfolgungsdatei herunterladen
- Herunterladen von Systeminformationen und Programmeinstellungen
- Ereignisprotokolle downloaden
- Erzeugen einer Dump-Datei für eine Anwendung
- Diagnose starten und Diagnoseberichte herunterladen
- Starten, Beenden und Neustart von Programmen

Sie können Ereignisprotokolle und Diagnoseberichte verwenden, die von einem Client-Gerät heruntergeladen wurden, um selbst Probleme zu beheben. Außerdem können Sie bei einer Anfrage an den Technischen Support von Kaspersky von einem Support-Experten aufgefordert werden, Protokolldateien, Dump-Dateien, Ereignisprotokolle und Diagnoseberichte von einem Client-Gerät für eine weitere Analyse bei Kaspersky herunterzuladen.

Öffnen des Fensters für die Ferndiagnose

Um die Ferndiagnose auf Windows- und Linux-basierten Client-Geräten durchzuführen, müssen Sie zunächst das Fenster für die Ferndiagnose öffnen.

So öffnen Sie das Fenster für die Ferndiagnose:

1. Führen Sie einen der folgenden Schritte aus, um das Gerät auszuwählen, für welches Sie das Ferndiagnosefenster öffnen möchten:

   - Wenn das Gerät zu einer Administrationsgruppe gehört, wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   - Wenn das Gerät zur Gruppe nicht zugeordneter Geräte gehört, wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Nicht zugeordnete Geräte**.

2. Klicken Sie auf den Namen des gewünschten Geräts.

3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Erweitert** aus.

4. Klicken Sie im folgenden Fenster auf **Remote-Diagnose**.

   Dies öffnet das Fenster **Remote-Diagnose** eines Client-Geräts. Wenn zwischen dem Administrationsserver und dem Client-Gerät keine Verbindung hergestellt werden kann, wird eine Fehlermeldung angezeigt.

Wenn Sie alternativ alle Diagnoseinformationen über ein Linux-basiertes Client-Gerät gleichzeitig abrufen möchten, können Sie auf diesem Gerät das Skript collect.sh ausführen.

Aktivieren und Deaktivieren der Ablaufverfolgung für Programme

Sie können die Ablaufverfolgung, einschließlich Xperf-Ablaufverfolgung, aktivieren und deaktivieren.

Ablaufverfolgung aktivieren und deaktivieren

Um die Ablaufverfolgung auf einem Remote-Gerät zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.

2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.

3. Wählen Sie in der Liste mit Programmen das Programm aus, für welches Sie die Ablaufverfolgung aktivieren oder deaktivieren möchten.

   Die Liste der Optionen zur Ferndiagnose wird geöffnet.

4. Wenn Sie die Ablaufverfolgung aktivieren möchten:

   a. Klicken Sie im Abschnitt **Ablaufverfolgung** auf **Ablaufverfolgung aktivieren**.

   b. Wir empfehlen Ihnen, im nächsten Fenster **Ablaufverfolgungsstufe ändern** die Standardwerte der Einstellungen beizubehalten. Bei Bedarf führt Sie ein Spezialist des Technischen Supports durch den Konfigurationsprozess. Es sind folgende Einstellungen verfügbar:

   - **Ablaufverfolgungsstufe**

     Die Ablaufverfolgungsstufe definiert die Detailstufe der Protokolldatei.

   - **Ablaufverfolgung auf Basis von Rotation**

     Die Anwendung überschreibt die Ablaufverfolgungsinformationen, um eine übermäßige Größenzunahme der Protokolldatei zu vermeiden. Geben Sie die maximale Anzahl von Dateien, die zum Speichern der Ablaufverfolgungsdaten verwendet werden sollen sowie die maximale Größe jeder Datei, an. Wenn die maximale Anzahl von Protokolldateien in maximaler Größe erreicht ist, wird die älteste Protokolldatei gelöscht, damit eine neue Protokolldatei erstellt werden kann.

     Diese Einstellung ist nur für Kaspersky Endpoint Security verfügbar.

   c. Klicken Sie auf die Schaltfläche **Speichern**.

   Die Ablaufverfolgung ist für das ausgewählte Programm aktiviert. In einigen Fällen ist es erforderlich, die Sicherheitsanwendungen und deren Aufgabe neu zu starten, um die Ablaufverfolgung zu aktivieren.

   Auf Linux-basierten Client-Geräten wird die Ablaufverfolgung der Komponente zum Aktualisieren des Administrationsagenten durch die Einstellungen des Administrationsagenten festgelegt. Daher sind die Optionen **Ablaufverfolgung aktivieren** und **Ablaufverfolgungsstufe ändern** für diese Komponente auf Linux-Client-Geräten deaktiviert.

5. Wenn Sie die Ablaufverfolgung für das ausgewählte Programm deaktivieren möchten, klicken Sie auf die Schaltfläche **Ablaufverfolgung deaktivieren**.

   Die Ablaufverfolgung ist für das ausgewählte Programm deaktiviert.

Aktivieren der Xperf-Ablaufverfolgung

Für Kaspersky Endpoint Security kann ein Spezialist des Technischen Supports Sie dazu auffordern, die Xperf-Ablaufverfolgung zu aktivieren, um Informationen über die Systemleistung zu erhalten.

So aktivieren, deaktivieren und konfigurieren Sie die Xperf-Ablaufverfolgung:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.

2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.

3. Wählen Sie in der Liste der Programme das Programm "Kaspersky Endpoint Security für Windows" aus.

   Die Liste mit Optionen zur Ferndiagnose für Kaspersky Endpoint Security für Windows wird angezeigt.

4. Klicken Sie im Abschnitt **Xperf-Ablaufverfolgung** auf **Xperf-Ablaufverfolgung aktivieren**.

   Wenn die Xperf-Ablaufverfolgung bereits aktiviert ist, wird stattdessen die Schaltfläche **Xperf-Ablaufverfolgung deaktivieren** angezeigt. Klicken Sie auf diese Schaltfläche, wenn Sie die Xperf-Ablaufverfolgung für Kaspersky Endpoint Security für Windows deaktivieren möchten.

5. Wählen Sie im nächsten Fenster **Xperf-Ablaufverfolgungsstufe ändern** eine der folgenden Ablaufverfolgungsstufen entsprechend den Anweisungen des Spezialisten des technischen Supports aus:

   a. Wählen Sie eine der folgenden Ablaufverfolgungsstufen aus:

   - **Leichte Stufe**

     Eine Protokolldatei dieses Typs enthält die Mindestmenge an Informationen über das System.

     Diese Variante ist standardmäßig ausgewählt.

   - **Tiefe Stufe**

     Eine Protokolldatei dieses Typs enthält detailliertere Informationen als Protokolldateien vom Typ *Leicht* und kann von den Experten des Technischen Supports angefordert werden, wenn eine Protokolldatei vom Typ *Leicht* nicht für die Beurteilung der Leistung ausreicht. Die Protokolldatei der Stufe *Tief* enthält technische Informationen zum System einschließlich: Informationen zur Hardware und zum Betriebssystem; Liste der gestarteten und abgeschlossenen Prozesse und Anwendungen; Ereignisse, die für die Leistungsbewertung verwendet wurden; Ereignisse aus dem Windows-Systembewertungstool.

   b. Wählen Sie eine der folgenden Xperf-Ablaufverfolgungstypen aus:

   - **Basistyp**

     Die Ablaufverfolgungsinformationen werden während der Ausführung der Sicherheitsanwendung Kaspersky Endpoint Security empfangen.

     Diese Variante ist standardmäßig ausgewählt.

   - **Bei-Neustart-Typ**

     Die Ablaufverfolgungsinformationen werden empfangen, während das Betriebssystem auf dem verwalteten Gerät gestartet wird. Diese Art von Ablaufverfolgung ist wirksam, wenn das Problem, das die Systemleistung beeinträchtigt, nach dem Einschalten des Geräts und vor dem Start von Kaspersky Endpoint Security auftritt.

   Sie werden möglicherweise auch aufgefordert, die Option **Größe der Dateien in Rotation, in MB** zu aktivieren, um eine übermäßige Größenzunahme der Protokolldateien zu vermeiden. Geben Sie dann die maximale Größe der Protokolldatei an. Wenn die Datei die maximale Größe erreicht, werden die ältesten Informationen der Ablaufverfolgung durch neue Informationen überschrieben.

   c. Legen Sie die Größe der Rotationsdatei fest.

   d. Klicken Sie auf die Schaltfläche **Speichern**.

   Die Xperf-Ablaufverfolgung ist aktiviert und konfiguriert.

6. Wenn Sie die Xperf-Ablaufverfolgung für Kaspersky Endpoint Security für Windows deaktivieren möchten, klicken Sie im Abschnitt **Xperf-Ablaufverfolgung** auf **Xperf-Ablaufverfolgung deaktivieren**.

   Die Xperf-Ablaufverfolgung ist deaktiviert.

Herunterladen der Protokolldateien eines Programms

Um eine Protokolldatei einer Anwendung herunterzuladen, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.
3. Wählen Sie in der Liste der Programme jenes aus, für das Sie die Protokolldatei herunterladen möchten.
4. Klicken Sie im Abschnitt **Ablaufverfolgung** auf **Protokolldateien**.

   Dadurch wird das Fenster **Ablaufverfolgungsprotokolle des Geräts** geöffnet, welches eine Liste von Protokolldateien anzeigt.
5. Wählen Sie in der Liste der Protokolldateien die Datei aus, die Sie herunterladen möchten.
6. Führen Sie eine der folgenden Aktionen aus:

   - Laden Sie die ausgewählte Datei durch Klicken auf **Herunterladen** herunter. Sie können mehrere Dateien zum Herunterladen auswählen.
   - Um einen Teil der ausgewählten Datei herunterzuladen:

     a. Klicken Sie auf die Schaltfläche **Einen Teil herunterladen**.

     Das gleichzeitige Herunterladen von Teilen mehrerer Dateien ist nicht möglich. Wenn Sie mehr als eine Protokolldatei auswählen, wird die Schaltfläche **Einen Teil herunterladen** deaktiviert.

     b. Geben Sie im folgenden Fenster den Namen und den herunterzuladenden Teil der Datei entsprechend Ihren Anforderungen an.

     Für Linux-basierte Geräte ist das ändern des Namens für Datei-Teile nicht verfügbar.

     c. Klicken Sie auf die Schaltfläche **Herunterladen**.

Die ausgewählte Datei oder deren Teil wird an den von Ihnen angegebenen Speicherort heruntergeladen.

Löschen der Protokolldateien

Sie können nicht mehr benötigte Protokolldateien löschen.

So löschen Sie eine Protokolldatei:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im folgenden Ferndiagnosefenster die Registerkarte **Ereignisprotokolle** aus.
3. Klicken Sie im Abschnitt **Protokolldateien** auf die Schaltfläche **Windows Update-Protokolle** oder **Protokolle von Remote-Installation**, je nachdem, welche Protokolldateien Sie löschen möchten.

Der Link **Windows Update-Protokolle** ist nur für Windows-basierte Client-Geräte verfügbar.

Dadurch wird das Fenster **Ablaufverfolgungsprotokolle des Geräts** geöffnet, welches eine Liste von Protokolldateien anzeigt.

4. Wählen Sie in der Liste der Protokolldateien die Dateien aus, die Sie löschen möchten.
5. Klicken Sie auf die Schaltfläche **Entfernen**.

Die ausgewählten Protokolldatei werden gelöscht.

Anwendungseinstellungen herunterladen

Um die Programmeinstellungen von einem Client-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Programme von Kaspersky** aus.
3. Klicken Sie im Abschnitt **Programmeinstellungen** auf die Schaltfläche **Herunterladen**, um Informationen über die Einstellungen der auf dem Client-Gerät installierten Anwendungen herunterzuladen.

Das zip-Archiv mit Informationen wird an den angegebenen Speicherort heruntergeladen.

Ereignisprotokolle downloaden

Um das Ereignisprotokoll von einem Remote-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Klicken Sie im Fenster "Ferndiagnose" auf der Registerkarte **Ereignisprotokolle** auf **Alle Geräteprotokolle**.
3. Wählen Sie im Fenster **Alle Geräteprotokolle** die erforderlichen Protokolle aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Laden Sie das ausgewählte Protokoll herunter, indem Sie auf **Vollständige Datei herunterladen** klicken.
   - Um einen Teil des ausgewählten Protokolls herunterzuladen:
     a. Klicken Sie auf die Schaltfläche **Einen Teil herunterladen**.

     Das gleichzeitige Herunterladen von Teilen mehrerer Protokolle ist nicht möglich. Wenn Sie mehr als ein Ereignisprotokoll auswählen, wird die Schaltfläche **Einen Teil herunterladen** deaktiviert.

b. Geben Sie im folgenden Fenster den Namen und den herunterzuladenden Teil des Protokolls entsprechend Ihren Anforderungen an.

Für Linux-basierte Geräte ist das ändern des Namens für Protokoll-Teile nicht verfügbar.

c. Klicken Sie auf die Schaltfläche **Herunterladen**.

Das ausgewählte Ereignisprotokoll oder ein Teil davon wird an den angegebenen Speicherort heruntergeladen.

Starten, Stoppen und Neustarten der Anwendung

Sie können Anwendungen auf einem Client-Gerät starten, stoppen und neu starten.

Um eine Anwendung zu starten, zu beenden oder neu zu starten, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.
3. Wählen Sie in der Liste der Programme das Programm aus, dass Sie starten, stoppen oder neu starten möchten.
4. Wählen Sie eine Aktion aus, indem Sie auf eine der folgenden Schaltflächen klicken:

   - **Programm beenden**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Programm neu starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Programm starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm derzeit nicht ausgeführt wird.

   Je nach ausgewählter Aktion wird das erforderliche Programm auf dem Client-Gerät gestartet, beendet oder neu gestartet.

Wenn Sie den Administrationsagenten neu starten, wird eine Meldung angezeigt, dass die aktuelle Verbindung des Geräts zum Administrationsserver unterbrochen wird.

Remote-Diagnose für den Kaspersky Security Center Administrationsagenten ausführen und Ergebnisse herunterladen

So starten Sie auf einem Remote-Gerät die Diagnose für den Kaspersky Security Center Administrationsagenten und laden die Ergebnisse herunter:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.
3. Wählen Sie in der Liste mit den Programmen den **Kaspersky Security Center Administrationsagenten** aus.

   Die Liste der Optionen zur Ferndiagnose wird geöffnet.
4. Klicken Sie im Abschnitt **Diagnosebericht** auf **Diagnose ausführen**.

   Dadurch wird der Ferndiagnoseprozess gestartet und ein Diagnosebericht erstellt. Wenn der Diagnoseprozess abgeschlossen ist, wird die Schaltfläche **Diagnosereport herunterladen** verfügbar.
5. Klicken Sie auf die Schaltfläche **Diagnosereport herunterladen**, um den Bericht herunterzuladen.

Der Bericht wird an den angegebenen Speicherort heruntergeladen.

Ausführen eines Programms auf einem Client-Gerät

Möglicherweise müssen Sie ein Programm auf dem Client-Gerät ausführen, wenn ein Spezialist des Technischen Supports von Kaspersky Sie dazu auffordert. Sie müssen das Programm nicht auf dem Gerät installieren.

Gehen Sie wie folgt vor, um ein Programm auf dem Client-Gerät auszuführen:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Remote-Ausführung einer Anwendung** aus.
3. Klicken Sie im Abschnitt **Programmdateien** auf die Schaltfläche **Durchsuchen**, um ein zip-Archiv auszuwählen, das die Anwendung enthält, die Sie auf dem Client-Gerät ausführen möchten.

   > Das zip-Archiv muss den Ordner mit dem Tool enthalten. In diesem Ordner befindet sich die ausführbare Datei, die auf einem Remote-Gerät ausgeführt werden soll.

   Bei Bedarf können Sie den Namen der ausführbaren Datei und die Befehlszeilenargumente angeben. Füllen Sie dazu die Felder **Archivierte ausführbare Datei, die auf einem Remote-Gerät ausgeführt werden soll** und **Befehlszeilenargumente** aus.
4. Klicken Sie auf die Schaltfläche **Hochladen und ausführen**, um die angegebene Anwendung auf einem Client-Gerät auszuführen.
5. Folgen Sie den Anweisungen des Experten vom Kaspersky-Support.

Erzeugen einer Dump-Datei für eine Anwendung

Mit einer Dump-Datei für eine Anwendung können Sie die Parameter der Anwendung anzeigen, die an einem bestimmten Zeitpunkt auf einem Client-Gerät ausgeführt wird. Diese Datei enthält auch Informationen über die Module, die für eine Anwendung geladen wurden.

Das Erstellen von Dump-Dateien wird für Linux-Geräte nicht unterstützt.

Um Dump-Dateien mittels Ferndiagnose zu erstellen, wird das Tool "kldumper" verwendet. Dieses Tool erstellt auf Anfrage der Spezialisten des Technischen Supports Dump-Dateien der Prozesse von Kaspersky-Anwendungen. Ausführliche Informationen über die Voraussetzungen zur Verwendung des kldumper-Tools finden Sie in der Wissensdatenbank von Kaspersky Security Center.

So erzeugen Sie eine Dump-Datei für eine Anwendung:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Remote-Ausführung einer Anwendung** aus.
3. Geben Sie im Abschnitt **Dump-Datei für den Prozess erstellen** die ausführbare Datei der Anwendung an, für die Sie eine Dump-Datei erstellen möchten.
4. Klicken Sie auf die Schaltfläche **Dump-Datei herunterladen**.

   Es wird ein Archiv mit der Dump-Datei für die angegebene Anwendung heruntergeladen.

   Wenn die angegebene Anwendung nicht auf dem Client-Gerät ausgeführt wird, ist der Ordner "result" im heruntergeladenen Archiv leer.

   Wenn die angegebene Anwendung ausgeführt wird, aber der Download mit einem Fehler fehlschlägt oder der Ordner "result" im heruntergeladenen Archiv leer ist, schlagen Sie in der Wissensdatenbank von Kaspersky Security Center nach.

Ferndiagnose auf einem Linux-basierten Client-Gerät ausführen

Kaspersky Security Center ermöglicht es Ihnen, grundlegende Diagnoseinformationen von einem Client-Gerät herunterzuladen. Alternativ können Sie die Diagnoseinformationen über ein Linux-basiertes Gerät mithilfe des Skripts "collect.sh" von Kaspersky abrufen. Dieses Skript wird auf dem zu diagnostizierenden Linux-basierten Client-Gerät ausgeführt und erstellt eine Datei, welche die Diagnoseinformationen, die Systeminformationen für dieses Gerät, die Ablaufverfolgungsdateien der Programme, die Geräteprotokolle und eine Dump-Datei für im Notfall beendete Anwendungen enthält.

Es wird empfohlen, das Skript "collect.sh" zu verwenden, um alle Diagnoseinformationen über das Linux-basierte Client-Gerät auf einmal abzurufen. Wenn Sie die Diagnoseinformationen per Fernzugriff über Kaspersky Security Center herunterladen, müssen Sie alle Abschnitte der Benutzeroberfläche für die Ferndiagnose durchlaufen. Zudem die Diagnoseinformationen für ein Linux-basiertes Gerät werden wahrscheinlich nicht vollständig abgerufen.

Wenn Sie die generierte Datei mit den Diagnoseinformationen an den Technischen Support von Kaspersky senden möchten, löschen Sie alle vertraulichen Informationen, bevor Sie die Datei senden.

Gehen Sie wie folgt vor, um die Diagnoseinformationen mithilfe des Skripts "collect.sh" von einem Linux-basierten Client-Gerät herunterzuladen:

1. Laden Sie das in das Archiv "collect.tar.gz" gepackte Skript "collect.sh" herunter.
2. Kopieren Sie das heruntergeladene Archiv auf das Linux-basierte Client-Gerät, das diagnostiziert werden soll.
3. Führen Sie den folgenden Befehl aus, um das Archiv "collect.tar.gz" zu entpacken:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Führen Sie den folgenden Befehl aus, um die Ausführungsrechte für das Skript anzugeben:

   ```
   # chmod +x collect.sh
   ```

5. Führen Sie das Skript "collect.sh" unter Verwendung eines Kontos mit Administratorrechten aus:

   ```
   # ./collect.sh
   ```

Eine Datei mit den Diagnoseinformationen wird generiert und im Ordner "/tmp/$HOST_NAME-collect.tar.gz" gespeichert.

Dateien aus Quarantäne und Backup herunterladen und löschen

Dieser Abschnitt enthält Informationen zum Herunterladen und Löschen von Dateien aus Quarantäne und Backup in der Kaspersky Security Center Web Console.

Dateien aus Quarantäne und Backup herunterladen

Sie können Dateien aus Quarantäne und Backup nur herunterladen, wenn eine der beiden Bedingungen erfüllt ist: Entweder ist die Option **Verbindung mit Administrationsserver nicht trennen** in den Geräteeinstellungen aktiviert, oder es wird ein Verbindungsgateway verwendet. Andernfalls ist der Download nicht möglich.

So speichern Sie die Kopie einer Datei aus der Quarantäne oder dem Backup auf einer Festplatte:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Kopie der Datei aus der Quarantäne speichern wollen, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Quarantäne**.

   - Wenn Sie eine Kopie der Datei aus dem Backup speichern möchten, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Backup**.

2. Wählen Sie in dem sich öffnenden Fenster eine Datei aus, die Sie herunterladen möchten und klicken Sie auf **Herunterladen**.

   Der Download wird gestartet. Eine Kopie der Datei, die sich in der Quarantäne des Client-Geräts befindet, wird im angegebenen Order gespeichert.

Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console ändern

Sie können die Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console auswählen.

So ändern Sie die Sprache der Benutzeroberfläche:

1. Gehen Sie im Hauptmenü zu **Einstellungen → Sprache**.

2. Wählen Sie eine der unterstützten Lokalisierungssprachen aus.

API-Referenzhandbuch

Dieses Kaspersky Security Center OpenAPI-Referenzhandbuch soll Sie bei den folgenden Aufgaben unterstützen:

- Automatisierung und Individualisierung. Sie können dadurch Aufgaben automatisieren, die nicht manuell über die Verwaltungskonsole ausgeführt werden sollen. Sie können außerdem individuelle Lösungen implementieren, die von der Verwaltungskonsole momentan noch nicht unterstützt werden. Beispielsweise können Sie Kaspersky Security Center OpenAPI dazu verwenden, Scripte zu erstellen und auszuführen, die das Entwickeln und Pflegen einer Struktur von Administrationsgruppen vereinfachen.

- Individuelle Entwicklung. Sie können beispielsweise eine alternative MMC-basierte Verwaltungskonsole mit einem geringeren Funktionsumfang für Ihre Kunden entwickeln.

Verwenden Sie im OpenAPI-Referenzhandbuch das Suchfeld auf der rechten Seite des Bildschirms, um die von Ihnen benötigten Informationen zu finden.

OPENAPI-REFERENZHANDBUCH

Skriptbeispiele

Das OpenAPI-Referenzhandbuch enthält Beispiele für die in der folgenden Tabelle aufgeführten Python-Skripts. Diese Beispiele zeigen, wie Sie OpenAPI-Methoden aufrufen und verschiedene Aufgaben zum Schutz Ihres Netzwerks automatisch ausführen können, z. B. das Erstellen einer "primär/sekundär"-Hierarchie, das Ausführen von Aufgaben in Kaspersky Security Center oder das Zuweisen von Verteilungspunkten. Sie können die Beispiele unverändert ausführen oder Ihre eigenen Skripts basierend auf den Beispielen erstellen.

Um die OpenAPI-Methoden aufzurufen und Skripte auszuführen:

1. Laden Sie das Archiv KlAkOAPI.tar.gz herunter. Dieses Archiv enthält das KlAkOAPI-Paket sowie Beispiele (Sie können diese aus dem Archiv oder dem OpenAPI-Referenzhandbuch kopieren). Das Archiv "KlAkOAPI.tar.gz" befindet sich ebenfalls im Installationsordner von Kaspersky Security Center.

2. Installieren Sie das Paket KlAkOAPI aus dem Archiv KlAkOAPI.tar.gz auf einem Gerät mit installiertem Administrationsserver.

   Sie können nur auf Geräten, auf denen der Administrationsserver und das Paket KlAkOAPI installiert sind, OpenAPI-Methoden aufrufen, Beispiele ausführen und eigene Skripte ausführen.

Benutzerszenarien und Beispiele für entsprechende Kaspersky Security Center OpenAPI-Methoden

Beispiel	Ziel des Beispiels	Szenario
Loggen von KlAkParams	Unter Verwendung der `KlAkParams` -Datenstruktur können Sie Daten extrahieren und verarbeiten. Das ist ein Beispiel für die Arbeit mit dieser Datenstruktur. Die Ausgabe des Beispiels kann auf verschiedene Weisen präsentiert werden. Sie können die Daten erhalten, um eine HTTP-Methode zu versenden, oder um Sie in Ihrem Code zu verwenden.	Überwachung und Berichterstattung
"Primär/Sekundär"-Hierarchie erstellen und löschen	Sie können einen sekundären Administrationsserver hinzufügen und so eine Hierarchie vom Typ "primär/sekundär" festlegen. Alternativ können Sie den sekundären Administrationsserver von der Hierarchie trennen.	• Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen • Administrationsserver-Hierarchie löschen

Beispiel	Ziel des Beispiels	Szenario
Erstellen der Gruppenhierarchie, basierend auf der Struktur der Active Directory-Einheit	Sie können eine Active Directory-Einheit abfragen und eine Hierarchie aus entdeckten Gerätegruppen erstellen.	Administrationsgruppen anlegen
Erstellen der Gruppenhierarchie, basierend auf der Struktur der gecachten Active Directory-Einheit	Sie können eine Hierarchie der Gruppen mit verwalteten Geräten erstellen, die auf der bereits im Voraus abgefragten Active Directory-Einheit basiert. Wenn neue Geräte erst nach der letzten Abfrage in der Active Directory erscheinen, werden diese der Gruppe nicht hinzugefügt, da sie nicht im Abfrageresultat gespeichert sind.	Administrationsgruppen anlegen
Netzwerklisten-Dateien mittels Verbindungs-Gateway auf das angegebene Gerät herunterladen	Unter Verwendung eines Verbindungs-Gateways können Sie sich mit dem Administrationsagenten des benötigten Geräts verbinden und anschließend die Datei mit der Netzwerkliste auf Ihr Gerät herunterladen.	Verteilungspunkte und Verbindungs-Gateways anpassen
Einen Lizenzschlüssel, der sich in der Datenverwaltung des primären Administrationsservers befindet, auf sekundären Administrationsservern installieren	Sie können sich mit dem primären Administrationsserver verbinden, von ihm einen erforderlichen Lizenzschlüssel herunterladen, und diesen Schlüssel an alle in der Hierarchie enthaltenen sekundären Administrationsserver weiterleiten.	Lizenzierung der verwalteten Anwendungen
Erstellen eines Berichts über gültige Benutzerberechtigungen	Sie können verschiedene Berichte erstellen. Unter anderem können Sie den Bericht über gültige Benutzerberechtigungen unter Verwendung dieses Beispiels erstellen. Dieser Bericht gibt die Berechtigungen eines Benutzers in Abhängigkeit seiner oder ihrer Gruppe und Rolle an. Sie können den Bericht in den folgenden Formaten herunterladen: HTML, PDF oder Excel.	Bericht erstellen und anzeigen
Eine Aufgabe für ein Gerät starten	Unter Verwendung eines Verbindungs-Gateways können Sie sich mit dem Administrationsagenten des benötigten Geräts verbinden und anschließend die notwendige Aufgabe starten.	Manuelles Starten einer Aufgabe
Erstellen von IP-Subnetzen, basierend auf Active Directory Sites and Services	Basierend auf der von Ihnen verwendeten Active Directory-Einheit können Sie ein IP-Subnetz erstellen. Das Beispiel startet die Abfrage des angegebenen IP-Bereichs und löscht gefundene Subnetze, um Konflikte mit einem neuen Subnetz zu vermeiden. Führen Sie dieses Beispiel daher nicht in Netzwerken aus, für die das Vorhandensein von Subnetzen ein wichtiger Punkt ist. Nach der Abfrage wechselt das Beispiel in das Active Directory, untersucht jedes darin enthaltene Gerät und erstellt das IP-Subnetz. Um dies zu tun, verwendet das Beispiel Masken und IP-Adressen von allen Geräten.	Netzwerkschutz konfigurieren
Registrieren von Verteilungspunkten für Geräte in einer Gruppe	Sie können verwalteten Geräten die Rolle eines Verteilungspunkts (früher bekannt als "Update-Agent") zuweisen.	Datenbanken und Anwendungen von Kaspersky aktualisieren
Alle Gruppen durchzählen	Sie können mit Administrationsgruppen verschiedene Aktionen ausführen. Das Beispiel zeigt Folgendes: • Eine ID der Root-Gruppe der "Verwalteten Geräte" abrufen • Durch die Gruppenhierarchie bewegen • Die vollständige, erweiterte Gruppenhierarchie, einschließlich ihrer Namen und Vierschachtelungen abrufen	Administrationsserver konfigurieren
Aufgaben durchzählen, Aufgabenstatistiken abfragen und Aufgaben ausführen	Die folgenden Informationen können Sie abfragen: • Verlauf des Aufgabenprozesses • Aktueller Aufgabenstatus • Anzahl der Aufgaben mir unterschiedlichen Statuswerten Sie können auch eine Aufgabe starten. Standardmäßig startet das Beispiel eine Aufgabe, nachdem es Statistiken ausgegeben hat.	Aufgabenausführung überwachen

Beispiel	Ziel des Beispiels	Szenario
Eine Aufgabe erstellen und ausführen	Sie können eine Aufgabe erstellen. Geben Sie in dem Beispiel die folgenden Aufgabenparameter an: • Typ • Art der Ausführung • Name • Gerätegruppe, auf welche die Aufgabe angewendet wird Standardmäßig erstellt das Beispiel eine Aufgabe des Typs "Nachricht anzeigen". Sie können diese Aufgabe für alle verwalteten Geräte des Administrationsservers ausführen. Bei Bedarf können Sie eigene Aufgabenparameter angeben.	Aufgaben erstellen
Lizenzschlüssel durchzählen	Sie können eine Liste mit allen aktiven Lizenzschlüsseln für Kaspersky-Anwendungen abrufen, die auf den verwalteten Geräten des Administrationsservers installiert sind. Die Liste enthält detaillierte Informationen über jeden Lizenzschlüssel, darunter Name, Typ oder Ablaufdatum.	Informationen zu verwendeten Lizenzschlüsseln anzeigen
Einen internen Benutzer erstellen und auffinden	Sie können ein Benutzerkonto zur weiteren Bearbeitung erstellen.	Auswählen des Benutzerkontos für den Start des Administrationsservers
Eine benutzerdefinierte Kategorie erstellen	Sie können eine Programmkategorie mit den benötigten Parametern erstellen.	Manuell zu erweiternde Programmkategorie erstellen
Benutzer mittels SrvView durchzählen	Sie können die Klasse SrvView verwenden, um detaillierte Informationen vom Administrationsserver abzufragen. Unter Verwendung dieses Beispiels können Sie unter anderem eine Liste der Benutzer abrufen.	Benutzerkonten verwalten

Anwendungen, die über OpenAPI mit Kaspersky Security Center interagieren

Einige Anwendungen können über OpenAPI mit Kaspersky Security Center interagieren. Zu solchen Anwendungen gehören beispielsweise Kaspersky Anti Targeted Attack Platform und Kaspersky Security for Virtualization. Dies kann auch ein von Ihnen entwickelte benutzerdefinierte Client-Anwendung auf Basis von OpenAPI sein.

Anwendungen, die über OpenAPI mit Kaspersky Security Center interagieren, verbinden sich mit dem Administrationsserver. Wenn Sie für die Verbindung mit dem Administrationsserver eine Allow-Liste mit IP-Adressen konfiguriert haben, fügen Sie die IP-Adressen von den Geräten hinzu, auf denen Anwendungen laufen, die Kaspersky Security Center OpenAPI verwenden. Weitere Informationen darüber, ob die von Ihnen verwendete Anwendung durch OpenAPI unterstützt wird, entnehmen Sie der Hilfe der entsprechenden Anwendung.

Bewährte Verfahren für Dienstanbieter

Dieser Abschnitt bietet Informationen darüber, wie Kaspersky Security Center konfiguriert und verwendet wird.

Dieser Abschnitt enthält Empfehlungen für die Bereitstellung, Einstellungen und Nutzung des Programms, sowie Möglichkeiten zur Lösung von typischen Problemen, die bei der Ausführung des Programms entstehen.

Planung der Bereitstellung für Kaspersky Security Center

Bei der Planung der Verteilung der Komponenten von Kaspersky Security Center im Unternehmensnetzwerk müssen die folgenden Faktoren beachtet werden:

- Gesamtzahl der Geräte
- Anzahl der MSP-Kunden

Ein Administrationsserver kann nicht mehr als 100.000 Geräte verwalten. Wenn die Gesamtzahl der Geräte im Unternehmensnetzwerk 100.000 überschreitet, müssen von Seiten des Anbieters mehrere Administrationsserver verteilt werden, die zur einfacheren zentralen Verwaltung in einer Hierarchie zusammengefasst sind.

Auf einem einzigen Administrationsserver können bis zu 500 virtuelle Server erstellt werden, was bedeutet, dass pro 500 MSP-Kunden ein separater Administrationsserver benötigt wird.

Bei der Planung der Bereitstellung muss die Notwendigkeit zur Angabe des speziellen X.509-Zertifikats für den Administrationsserver in Betracht gezogen werden. Die Zuweisung des X.509-Zertifikates für den Administrationsserver kann in folgenden Fällen (unvollständige Liste) hilfreich sein:

- Zur Untersuchung des SSL-Datenverkehrs (Secure Socket Layer) über SSL Termination Proxy
- Zur Angabe der gewünschten Werte für die Felder des Zertifikats
- Zur Gewährleistung der erwünschten Verschlüsselungsstärke des Zertifikats

Internetzugriff für den Administrationsserver bereitstellen

Damit die Geräte, die sich im Netzwerk des Kunden befinden, über das Internet mit dem Administrationsserver interagieren können, müssen die folgenden Ports des Administrationsservers verfügbar sein:

- 13000 TCP – TLS-Port des Administrationsservers zur Verbindung der im Kundennetzwerk bereitgestellten Administrationsagenten
- 8061 TCP – HTTPS-Port, der für die Veröffentlichung von autonomen Paketen mittels Verwaltungskonsole verwendet wird
- 806 TCP – HTTP-Port, der für die Veröffentlichung von autonomen Paketen mittels Verwaltungskonsole verwendet wird
- 13292 TCP – dieser TLS-Port wird nur für die Verwaltung von mobilen Geräten benötigt

Falls der Kunde grundlegende Möglichkeiten zur Verwaltung des eigenen Netzwerks mittels Kaspersky Security Center Web Console haben soll, müssen Sie auch den Port 8080 TCP (HTTPS-Port) der Kaspersky Security Center Web Console öffnen.

Typische Konfiguration von Kaspersky Security Center

Auf den MSP-Servern sind ein oder mehrere Administrationsserver vorhanden. Die Anzahl der Administrationsserver kann sowohl ausgehend von der vorhandenen verfügbaren Hardware als auch in Abhängigkeit von der Gesamtmenge der verwalteten MSP-Kunden oder der Gesamtmenge der verwalteten Geräte ausgewählt werden.

Ein Administrationsserver kann bis zu 100.000 Geräte verwalten. Die Möglichkeit einer Erhöhung der Anzahl der verwalteten Geräte in nächster Zukunft muss berücksichtigt werden: es kann sich als wünschenswert erweisen, eine etwas kleinere Anzahl von Geräten mit einem Administrationsserver zu verbinden.

Auf einem einzigen Administrationsserver können bis zu 500 virtuelle Server erstellt werden, was bedeutet, dass pro 500 MSP-Kunden ein separater Administrationsserver benötigt wird.

Wenn es mehrere Server gibt, ist es empfehlenswert, sie in einer Hierarchie zusammenzufassen. Das Verwenden einer Hierarchie der Administrationsserver erlaubt Ihnen, das Duplizieren von Richtlinien und Aufgaben zu vermeiden und mit allen verwalteten Geräte zu arbeiten, als ob sie von einem Administrationsserver verwaltet würden: Geräte suchen, Geräteauswahlen erstellen, Berichte erstellen.

Auf jedem virtuellen Server, der dem MSP-Kunden entspricht, müssen ein oder mehrere Verteilungspunkte bestimmt werden. Wenn die Verbindung zwischen den MSP-Kunden und dem Administrationsserver über das Internet hergestellt wird, kann es sinnvoll sein, für die Verteilungspunkte die *Aufgabe zum Download von Updates in die Datenverwaltung von Verteilungspunkten* zu erstellen, damit die Verteilungspunkte die Updates nicht vom Administrationsserver, sondern direkt von den Kaspersky-Servern herunterladen.

Wenn ein Teil der Geräte im Netzwerk des MSP-Kunden keinen direkten Internetzugang besitzt, müssen die Verteilungspunkte in den Gateway-Modus (Connection Gateway) versetzt werden. In diesem Fall werden die Administrationsagenten auf den Geräten im Netzwerk des MSP-Kunden (zwecks Synchronisierung) nicht direkt, sondern über ein Gateway mit dem Administrationsserver verbunden.

Da der Administrationsserver das Netzwerk des MSP-Kunden höchstwahrscheinlich nicht abfragen kann, ist es sinnvoll, das Ausführen dieser Funktion auf einen der Verteilungspunkte zu übertragen.

Der Administrationsserver kann an verwaltete Geräte, die sich im Netzwerk des MSP-Kunden hinter NAT befinden, keine Benachrichtigungen an den Port 15000 UDP senden. Für die Behebung dieses Problems ist es sinnvoll, in den Eigenschaften der Geräte, die als Verteilungspunkte dienen und die im Gateway-Modus ausgeführt werden (Connection Gateway), den Modus zur ständigen Verbindung mit dem Administrationsserver (Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**) zu aktivieren. Der Modus der ständigen Verbindung ist verfügbar, wenn die Gesamtanzahl der Verteilungspunkte 300 nicht überschreitet.

Über Verteilungspunkte

Ein Gerät mit Administrationsagent kann als Verteilungspunkt verwendet werden. In diesem Modus kann der Administrationsagent folgende Tätigkeiten ausführen:

- Dateien an Client-Geräte übertragen, einschließlich:
  - Updates für die Datenbanken und Programm-Module von Kaspersky

    Die Updates können sowohl vom Administrationsserver als auch von den Kaspersky-Servern abgerufen werden. Im zweiten Fall muss für das Gerät, das als Verteilungspunkt dient, die Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* erstellt werden.
  - Updates für Drittanbieter-Programme
  - Installationspakete
  - Windows-Updates, wenn Sie Administrationsserver als WSUS-Server verwenden
- Software auf anderen Geräten installieren, einschließlich Ausführung der erstmaligen Bereitstellung der Administrationsagenten auf den Geräten.
- Das Netzwerk abfragen, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden. Der Verteilungspunkt kann dieselben Methoden zur Gerätesuche ausführen wie der Administrationsserver.

Die Bereitstellung von Verteilungspunkten im Unternehmensnetzwerk verfolgt die folgenden Ziele:

- Reduzierung der Auslastung des Administrationsservers in dem Fall, dass der Administrationsserver als Update-Quelle dient.
- Optimierung des Internet-Datenverkehrs, da sich in diesem Fall nicht jedes Gerät im Netzwerk des MSP-Kunden an die Server von Kaspersky oder an den Administrationsserver wenden muss, um Updates zu erhalten.
- Wenn dem Administrationsserver der Zugriff auf die Geräte hinter der NAT (vom Standpunkt des Administrationsservers aus) des Netzwerks des MSP-Kunden gewährt wird, kann der Administrationsserver folgende Aktionen durchführen:
  - Nachrichten an Geräte in IPv4- oder IPv6-Netzwerken über UDP versenden
  - Das IPv4- oder IPv6-Netzwerk abfragen
  - Erstmalige Bereitstellung ausführen
  - Als Push-Server fungieren

Ein Verteilungspunkt wird für eine Administrationsgruppe bestimmt. In diesem Fall umfasst der Gültigkeitsbereich für den Verteilungspunkt alle Geräte, die sich in einer solcher Administrationsgruppe und allen ihren Untergruppen befinden. Dabei muss sich das Gerät, das als Verteilungspunkt fungiert, nicht in der Administrationsgruppe befinden, für die es bestimmt wurde.

Sie können einen Verteilungspunkt als Verbindungs-Gateway nutzen. Die Geräte, die sich in diesem Verteilungspunkt befinden, werden in diesem Fall nicht direkt, sondern durch ein Gateway mit dem Administrationsserver verbunden. Der vorliegende Modus ist in Szenarien nützlich, bei denen zwischen den Geräten mit dem Administrationsagenten und dem Administrationsserver keine direkte Verbindung möglich ist.

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Hierarchie des Administrationsservers

Beim MSP kann mehr als ein Administrationsserver vorhanden sein. Die Verwaltung mehrerer vereinzelter Administrationsserver ist unpraktisch, deshalb es ist zweckmäßig, sie in einer Hierarchie zusammenzufassen. Eine "Primär/Sekundär"-Konfiguration für zwei Administrationsserver bietet die folgenden Möglichkeiten:

- Der sekundäre Administrationsserver erbt vom primären Administrationsserver die Richtlinien und Aufgaben, wobei duplizierte Einstellungen entfernt werden.
- Die Geräteauswahlen auf dem primären Administrationsserver können Geräte der sekundären Administrationsserver einschließen.
- Die Berichte auf dem primären Administrationsserver können Daten (einschließlich ausführlicher Informationen) der sekundären Administrationsserver einschließen.

Der primäre Administrationsserver empfängt Daten von sekundären Administrationsservern, die nicht virtuell sind, nur im Rahmen der oben aufgeführten Optionen. Diese Einschränkung gilt nicht für virtuelle Administrationsserver, welche die Datenbank mit ihrem primären Administrationsserver teilen.

Virtuelle Administrationsserver

Im Rahmen des physischen Administrationsservers können mehrere virtuelle Administrationsserver erstellt werden, die in vieler Hinsicht sekundären Servern ähnlich sind. Im Vergleich zum Modell des geteilten Zugriffs, der auf den Listen der Zugriffskontrolle (ACL) beruht, ist das Modell der virtuellen Administrationsserver funktioneller und bietet eine hohe Stufe der Isolierung. Neben der eigenen Struktur der Administrationsgruppen für verwaltete Geräte mit Richtlinien und Aufgaben hat jeder virtuelle Administrationsserver auch eine eigene Gruppe von nicht zugeordneten Geräten, die über eigene Sätze von Berichten, Geräteauswahlen und Ereignissen, Installationspakete, Regeln zur Verschiebung von Geräten usw. verfügt. Um MSP-Kunden bestmöglich voneinander zu isolieren, wird empfohlen, die Funktionalität virtueller Administrationsserver zu verwenden. Außerdem ermöglicht das Erstellen eines virtuellen Administrationsservers für jeden MSP-Kunden, den Kunden grundlegende Möglichkeiten zur Verwaltung des eigenen Netzwerkes mittels Kaspersky Security Center Web Console zu gewähren.

Virtuelle Administrationsserver ähneln in vieler Hinsicht sekundären Administrationsservern, haben jedoch die folgenden Unterschiede:

- Einem virtuellen Administrationsserver fehlt eine Vielzahl der globalen Einstellungen und eigenen TCP-Ports
- Ein virtueller Administrationsserver hat keine sekundären Administrationsserver
- Ein virtueller Administrationsserver kann keine eigenen virtuellen Administrationsserver haben

- Auf dem physischen Administrationsserver sind die Geräte, Gruppen, Ereignisse und Objekte der verwalteten Geräte (Elemente der Quarantäne, Programm-Registry und andere) aller seiner virtuellen Administrationsserver sichtbar
- Ein virtueller Administrationsserver kann das Netzwerk nur mittels der mit ihm verbundenen Verteilungspunkte abfragen

Mobile Geräte mit installiertem Kaspersky Endpoint Security für Android verwalten

Die Verwaltung von mobilen Geräten mit installierter App Kaspersky Endpoint Security für Android™ (im Weiteren KES-Geräte) erfolgt mithilfe des Administrationsservers. Kaspersky Security Center unterstützt die folgenden Funktionen zur Verwaltung von KES-Geräten:

- Arbeit mit mobilen Geräten und den Client-Geräten:
  - Zugehörigkeit zu Administrationsgruppen
  - Überwachung, z. B. Anzeigen von Statuswerten, Ereignissen und Berichten
  - Änderung der lokalen Einstellungen und Festlegung der Richtlinie für die App Kaspersky Endpoint Security für Android
- Zentralisierter Versand von Befehlen
- Remote-Installation der Pakete mit mobilen Anwendungen

Der Administrationsserver verwaltet KES-Geräte über TLS, TCP-Port 13292.

Bereitstellung und Erstkonfiguration

Kaspersky Security Center ist ein verteiltes Programm. Im Lieferumfang von Kaspersky Security Center sind folgende Komponenten enthalten:

- Administrationsserver – die zentrale Komponente, die für die Verwaltung der Geräte des Unternehmens und für die Datenspeicherung im DBMS verantwortlich ist.
- Verwaltungskonsole – das grundlegende Werkzeug des Administrators. Die Verwaltungskonsole wird zusammen mit dem Administrationsserver geliefert, kann aber auch separat auf einem oder mehreren Geräten des Administrators installiert sein.
- Kaspersky Security Center Web Console — Webschnittstelle zum Administrationsserver für die Ausführung grundlegender Vorgänge. Sie können diese Komponente auf jedem Gerät installieren, das die Hard- und Softwarevoraussetzungen erfüllt.
- Administrationsagent – dient zur Verwaltung der auf einem Gerät installierten Sicherheitsanwendungen sowie zum Empfangen von Informationen über dieses Gerät. Die Administrationsagenten werden auf den Geräten des Unternehmens installiert.

Die Bereitstellung von Kaspersky Security Center im Netzwerk des Unternehmens verläuft auf folgende Weise:

- Installation des Administrationsservers
- Installation der Kaspersky Security Center Web Console
- Installation der Verwaltungskonsole auf dem Gerät des Administrators
- Installation des Administrationsagenten und der Sicherheitsanwendung auf den Geräten des Unternehmens

Installationsempfehlungen für den Administrationsserver

Dieser Abschnitt enthält Empfehlungen in Bezug auf die Installation des Administrationsservers. Im Abschnitt finden Sie ferner Szenarien für die Nutzung des freigegebenen Ordners auf dem Gerät mit dem Administrationsserver zur Bereitstellung des Administrationsagenten auf den Client-Geräten.

Benutzerkonten für die Dienste des Administrationsservers auf dem Failover-Cluster erstellen

Standardmäßig erstellt der Installer selbständig keine nicht privilegierten Benutzerkonten für die Dienste des Administrationsservers. Dieses Verhalten eignet sich am besten für die Installation des Administrationsservers auf einem gewöhnlichen Gerät.

Bei der Installation des Administrationsservers auf einem störungssicheren Cluster muss jedoch anders vorgegangen werden:

1. Die nicht privilegierten Domänenbenutzerkonten für die Dienste des Administrationsservers erstellen und zu Mitgliedern der globalen Domänensicherheitsgruppe KLAdmins machen.
2. Im Installer des Administrationsservers die erstellten Domänenbenutzerkonten für Dienste festlegen.

Auswahl des DBMS

Bei der Auswahl des DBMS, das vom Administrationsserver verwendet wird, muss von der Anzahl der Geräte ausgegangen werden, die der Administrationsserver betreut.

In der nachfolgenden Tabelle sind die zulässigen DBMS-Varianten und deren Empfehlungen und Einschränkungen zur Verwendung aufgeführt.

DBMS	Empfehlungen und Einschränkungen
SQL Server Express Edition 2016 und höher.	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 10.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Sie können die maximale Anzahl an Ereignissen in der Ereignisverwaltung begrenzen, um ein Überlaufen der Datenbank zu verhindern. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank. Die gleichzeitige Verwendung des DBMS von SQL Server Express Edition durch den Administrationsserver und eine weitere Anwendung ist unzulässig. Die Microsoft SQL Express-Datenbank wird für die Aufgabe **Windows-Updates synchronisieren** nicht unterstützt.
SQL Server Edition (keine Express Edition), 2016 und höher, lokale Bereitstellung	Keine Einschränkungen.
SQL Server Edition (keine Express Edition), 2016 und höher, Remote-Bereitstellung	Nur gültig, wenn sich beide Geräte in derselben Windows®-Domäne befinden. Wenn die Domänen unterschiedlich sind, muss zwischen ihnen eine wechselseitige Vertrauensstellung hergestellt werden.
MySQL 5.5, 5.6 oder 5.7 (die MySQL Versionen 5.5.1, 5.5.2, 5.5.3, 5.5.4 und 5.5.5 werden nicht mehr unterstützt), lokale oder Remote-Bereitstellung	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 10.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.
MySQL 8.0.20 oder höher, lokale oder Remote-Bereitstellung	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.
MariaDB (siehe unterstützte Versionen), lokale oder Remote-Bereitstellung	Verwenden Sie dieses DBMS, wenn Sie einen Administrationsserver für bis zu 20.000 Geräte verwenden möchten. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.
PostgreSQL, Postgres Pro (siehe unterstützte Versionen)	Verwenden Sie eins dieser DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen. Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren. Ausführliche Informationen finden Sie im folgenden Thema: Berechnung des Speicherplatzes in der Datenbank.

Wenn Sie MSSQL 2019 auswählen, müssen Sie den kumulativen Patch CU12 oder höher verwenden. Dadurch können Sie auftretende Fehler und eine Systemüberlastung vermeiden.

Wenn Sie PostgreSQL, MariaDB oder MySQL als DBMS verwenden, wird auf der Registerkarte **Ereignisse** möglicherweise eine unvollständige Liste der Ereignisse für das ausgewählte Client-Gerät angezeigt. Dies kommt vor, wenn das DBMS eine sehr große Anzahl von Ereignissen speichert. Sie können die Anzahl der angezeigten Ereignisse auf eine der folgenden Arten erhöhen:

- Nicht benötigte Ereignisse entfernen.
- Speicherdauer für nicht benötigte Ereignisse verkürzen.

Verwenden Sie die Berichte, um eine vollständige Liste der auf dem Administrationsserver für das Gerät protokollierten Ereignisse anzuzeigen.

Adresse des Administrationsservers angeben

Bei der Installation des Administrationsservers muss die externe Adresse des Administrationsservers festgelegt werden. Diese Adresse wird standardmäßig beim Erstellen der Installationspakete des Administrationsagenten verwendet. In Folge kann die Adresse des Hosts des Administrationsservers mithilfe der Verwaltungskonsole geändert werden, dabei wird er jedoch wird nicht automatisch in den schon erstellten Installationspaketen des Administrationsagenten geändert.

Schutz im Netzwerk eines Kundenunternehmens anpassen

Nach dem Abschließen der Installation des Administrationsservers wird die Verwaltungskonsole gestartet und diese schlägt vor, mithilfe des Assistenten die Erstkonfiguration auszuführen. Während der Ausführung des Schnellstartassistenten in der Stamm-Administrationsgruppe werden die folgenden Richtlinien und Aufgaben erstellt:

- Richtlinie von Kaspersky Endpoint Security
- Gruppenaufgabe zum Update von Kaspersky Endpoint Security
- Gruppenaufgabe zur Untersuchung des Geräts von Kaspersky Endpoint Security
- Richtlinie für den Administrationsagenten
- Aufgabe zur Untersuchung auf Schwachstellen (Aufgabe des Administrationsagenten)
- Aufgabe zur Installation der Updates und zum Schließen von Schwachstellen (Aufgabe des Administrationsagenten)

Die Richtlinien und Aufgaben werden mit den Standardeinstellungen erstellt, die sich möglicherweise als nicht optimal oder sogar untauglich für das vorliegende Unternehmen erweisen. Deshalb ist es erforderlich, die Eigenschaften der erstellten Objekte anzuzeigen erforderlichenfalls manuelle Änderungen vorzunehmen.

Dieser Abschnitt enthält Informationen über die manuelle Konfiguration von Richtlinien, Aufgaben und andere Einstellungen des Administrationsservers sowie Informationen über den Verteilungspunkt, den Aufbau der Struktur der Administrationsgruppen, die Hierarchie von Aufgaben und andere Einstellungen.

Richtlinie für Kaspersky Endpoint Security manuell konfigurieren

Dieser Abschnitt enthält Empfehlungen für das Anpassen der Einstellungen der Richtlinie für Kaspersky Endpoint Security, die vom Schnellstartassistenten erstellt wird. Sie können die Einrichtung im Fenster mit den Richtlinieneigenschaften durchführen.

Beachten Sie beim Ändern einer Einstellung, dass Sie über der entsprechenden Einstellung auf die Schaltfläche mit dem "Schloss" klicken müssen, um den Einstellungswert auf der Workstation zu verwenden.

Einstellungen der Richtlinie im Abschnitt "Erweiterter Schutz"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

Im Abschnitt **Erweiterter Schutz** können Sie die Verwendung von Kaspersky Security Network für Kaspersky Endpoint Security für Windows anpassen. Sie können auch die Module von Kaspersky Endpoint Security für Windows anpassen. Dazu zählen "Verhaltensanalyse", "Exploit-Prävention", "Programm-Überwachung" und "Rollback von schädlichen Aktionen".

Es wird empfohlen, im Unterabschnitt **Kaspersky Security Network** die Option **Kaspersky Security Network** zu aktivieren. Diese Option unterstützt Sie bei der Umverteilung und Optimierung des Datenverkehrs im Netzwerk. Wenn die Option **Kaspersky Security Network** deaktiviert ist, können Sie die direkte Verwendung von KSN-Servern aktivieren.

Einstellungen der Richtlinie im Abschnitt "Basisschutz"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

Es wird empfohlen, dass Sie im Abschnitt **Basisschutz** des Eigenschaftsfensters der Richtlinie die zusätzlichen Einstellungen für die Unterabschnitte **Firewall** und **Schutz vor bedrohlichen Dateien** angeben.

Der Unterabschnitt **Firewall** enthält Einstellungen, mit denen Sie die Netzwerkaktivität von Anwendungen auf den Client-Geräten steuern können. Ein Client-Gerät verwendet ein Netzwerk, dem einer der folgenden Statuswerte zugewiesen ist: öffentlich, lokal oder vertrauenswürdig. Je nach Netzwerkstatus kann Kaspersky Endpoint Security die Netzwerkaktivitäten auf einem Gerät zulassen oder verweigern. Wenn Sie Ihrer Organisation ein neues Netzwerk hinzufügen, müssen Sie ihm einen entsprechenden Netzwerkstatus zuweisen. Wenn das Client-Gerät beispielsweise ein Laptop ist, empfehlen wir, dass dieses Gerät das öffentliche oder vertrauenswürdige Netzwerk verwendet, da der Laptop nicht ausschließlich mit dem lokalen Netzwerk verbunden ist. In dem Unterabschnitt **Firewall** können Sie überprüfen, ob Sie die Statuswerte der in Ihrer Organisation verwendeten Netzwerke korrekt zugewiesen haben.

Um die Liste der Netzwerke zu überprüfen, gehen Sie wie folgt vor:

1. Wechseln Sie in den Richtlinieneinstellungen zu Basisschutz → **Firewall**.
2. Klicken Sie im Block **Verfügbare Netzwerke** auf die Schaltfläche **Einstellungen**.
3. Wechseln Sie im angezeigten Fenster **Firewall** zu der Registerkarte **Netzwerke**, um die Liste der Netzwerke anzuzeigen.

In dem Unterabschnitt **Schutz vor bedrohlichen Dateien** können Sie das Untersuchen von Netzlaufwerken deaktivieren. Das Untersuchen von Netzlaufwerken kann eine erhebliche Belastung auf den Netzlaufwerken darstellen. Daher ist es zweckmäßiger, die Untersuchung unmittelbar auf den Dateiservern auszuführen.

Um die Untersuchung von Netzlaufwerken zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie in den Richtlinieneinstellungen zu **Basisschutz → Schutz vor bedrohlichen Dateien**.
2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf **Einstellungen**.
3. Deaktivieren Sie neuen Fenster **Schutz vor bedrohlichen Dateien** auf der Registerkarte **Allgemein** das Kontrollkästchen **Alle Netzlaufwerke**.

Einstellungen der Richtlinie im Abschnitt "Allgemeine Einstellungen"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security.

Es folgt die Beschreibung der erweiterten Einrichtung anhand von Maßnahmen, die im Eigenschaftenfenster der Richtlinie von Kaspersky Endpoint Security im Abschnitt **Allgemeine Einstellungen** durchgeführt werden sollten.

Abschnitt "Allgemeine Einstellungen", Unterabschnitt "Berichte und Speicher"

Bitte beachten Sie im Abschnitt **Datenübertragung zum Administrationsserver** das Kontrollkästchen **Über gestartete Anwendungen**. Wenn dieses Kontrollkästchen aktiviert ist, werden in der Administrationsserver-Datenbank Informationen über alle Versionen aller Programm-Module auf den Geräten im Unternehmensnetzwerk gespeichert. Diese Informationen können in der Datenbank von Kaspersky Security Center eine erhebliche Größe (mehrere Gigabyte) einnehmen. Wenn daher das Kontrollkästchen **Über die ausgeführten Programme** in der Richtlinie der obersten Ebene noch aktiviert ist, muss es dort deaktiviert werden.

Abschnitt "Allgemeine Einstellungen", Unterabschnitt "Benutzeroberfläche"

Wenn der Bedrohungsschutz im Unternehmensnetzwerk zentral über die Verwaltungskonsole verwaltet werden soll, müssen Sie die Anzeige der Benutzeroberfläche von Kaspersky Endpoint Security auf den Workstations deaktivieren (Deaktivieren des Kontrollkästchen **Benutzeroberfläche anzeigen** im Abschnitt **Interaktion mit dem Benutzer**) und den Kennwortschutz aktivieren (Aktivieren des Kontrollkästchens **Kennwortschutz aktivieren** im Abschnitt **Kennwortschutz**).

Einstellungen der Richtlinie im Abschnitt "Konfiguration von Ereignissen"

Im Abschnitt **Konfiguration von Ereignissen** muss die Speicherung aller Ereignisse auf dem Administrationsserver mit Ausnahme der nachstehenden deaktiviert werden:

- Auf der Registerkarte **Kritisch**:
  - *Autostart des Programms wurde deaktiviert*
  - *Zugriff verweigert*
  - *Programmstart verboten*
  - *Desinfektion nicht möglich*
  - *Endbenutzer-Lizenzvertrag wurde verletzt*

- *Das Verschlüsselungsmodul konnte nicht geladen werden*
- *Zwei Aufgaben können nicht gleichzeitig gestartet werden*
- *Eine aktive Bedrohung wurde gefunden. Die aktive Desinfektion muss gestartet werden*
- *Netzwerkangriff erkannt*
- *Nicht alle Komponenten wurden aktualisiert*
- *Aktivierungsfehler*
- *Fehler beim Aktivieren des portablen Modus*
- *Fehler bei Interaktion mit Kaspersky Security Center*
- *Fehler beim Deaktivieren des portablen Modus*
- *Fehler beim Ändern der Auswahl der Programmkomponenten*
- *Fehler bei der Anwendung von Regeln zur Verschlüsselung / Entschlüsselung von Dateien*
- *Die Richtlinie kann nicht übernommen werden*
- *Prozess beendet*
- *Netzwerkaktivität verboten*

- Auf der Registerkarte **Funktionsfehler**: *Ungültige Aufgabeneinstellungen. Einstellungen nicht übernommen*
- Auf der Registerkarte **Warnung**:
  - *Selbstschutz ist deaktiviert*
  - *Ungültiger Reserveschlüssel*
  - *Der Benutzer hat die Verschlüsselungsrichtlinie abgelehnt*
- Auf der Registerkarte **Information**: *Programmstart im Testmodus verboten*

Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren

Falls der Administrationsserver als Update-Quelle dient, ist der Zeitplan **Nach dem Download von Updates in die Datenverwaltung** bei aktiviertem Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** der optimale und empfohlene Zeitplan für Gruppenaufgaben zum Update von Kaspersky Endpoint Security.

Wenn Sie auf jedem Verteilungspunkt eine lokale Aufgabe für den Download von Updates von den Servern von Kaspersky in den Speicher erstellt haben, ist für die Gruppenaufgabe zum Update von Kaspersky Endpoint Security ein regelmäßiger Zeitplan optimal und empfohlen. In diesem Fall sollte als Zeitraum für den zufälligen Start 1 Stunde angegeben werden.

Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security

Der Schnellstartassistent erstellt die Gruppenaufgabe zur Untersuchung des Geräts. Standardmäßig ist für die Aufgabe der Zeitplan **Donnerstags um 19:00 Uhr starten** mit automatischer Randomisierung ausgewählt und das Kontrollkästchen **Übersprungene Aufgaben starten** ist deaktiviert.

Wenn die Geräte des Unternehmens freitags, beispielsweise um 18:30 deaktiviert werden, bedeutet das, dass die Untersuchungsaufgabe des Geräts niemals ausgeführt wird. Es ist erforderlich, den optimalen Zeitplan dieser Aufgabe ausgehend von den im Unternehmen geltenden Dienstvorschriften zu konfigurieren.

Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen

Der Schnellstartassistent erstellt für den Administrationsagenten die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*. Standardmäßig ist für die Aufgabe der Zeitplan **Dienstag um 19:00 Uhr starten** mit automatischer Randomisierung ausgewählt und das Kontrollkästchen **Übersprungene Aufgaben starten** ist aktiviert.

Wenn die Dienstvorschriften des Unternehmens zu dieser Zeit ein Deaktivieren der Geräte vorsehen, wird die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* nach dem Aktivieren des Geräts (am Mittwochmorgen) ausgeführt. Ein solches Verhalten kann unerwünscht sein, da die Untersuchung auf Schwachstellen eine erhöhte Belastung des Prozessors und des Laufwerkssubsystems des Geräts veranlassen kann. Für einen optimalen Aufgabenzeitplan sollten die im Unternehmen geltenden Regeln und Vorschriften berücksichtigt werden.

Manuelle Konfiguration der Gruppenaufgabe zur Installation von Updates und zum Schließen von Schwachstellen

Der Schnellstartassistent erstellt für den Administrationsagenten die Gruppenaufgabe zur Installation der Updates und zum Schließen von Schwachstellen. Standardmäßig ist der Aufgabenstart täglich um 1:00 Uhr mit zufälliger Verzögerung konfiguriert und die Option **Übersprungene Aufgaben starten** ist deaktiviert.

Wenn die Dienstvorschriften des Unternehmens während der Nacht ein Deaktivieren der Geräte vorsehen, wird die Aufgabe zur Installation der Updates niemals ausgeführt. Es ist erforderlich, den optimalen Zeitplan der Aufgabe zur Untersuchung auf Schwachstellen ausgehend von den im Unternehmen geltenden Dienstvorschriften festzulegen. Ferner muss berücksichtigt werden, dass infolge der Installation der Updates ein Neustart des Geräts erforderlich sein kann.

Aufbau der Struktur von Administrationsgruppen und Zuweisung von Verteilungspunkten

Die Struktur der Administrationsgruppen in Kaspersky Security Center erfüllt folgende Funktionen:

- Gültigkeitsbereich der Richtlinien festlegen.

  Mithilfe von Richtlinienprofilen existiert eine alternative Möglichkeit, um die notwendigen Einstellungen auf den Geräten anzuwenden. In diesem Fall wird der Gültigkeitsbereich der Richtlinien z. B. mittels Tags, des Speicherorts der Geräte in den Active Directory-Verzeichnissen und der Zugehörigkeit zu den Active Directory-Sicherheitsgruppen festgelegt.

- Gültigkeitsbereich der Gruppenaufgaben festlegen.

  Es gibt eine Methode zur Festlegung des Gültigkeitsbereichs der Gruppenaufgaben, die nicht auf der Hierarchie der Administrationsgruppen basiert: die Nutzung von Aufgaben für die Geräteauswahlen und eine Reihe von Geräten.

- Festlegung der Zugriffsrechte auf die Geräte, die virtuellen und sekundären Administrationsserver.

- Weist Verteilungspunkte zu.

Beim Aufbau der Struktur der Administrationsgruppen muss für eine optimale Bestimmung der Verteilungspunkte die Netzwerktopologie des Unternehmens berücksichtigt werden. Die optimale Zuordnung der Verteilungspunkte ermöglicht eine Verringerung des Netzwerkverkehrs innerhalb des Unternehmensnetzwerks.

Abhängig von der planmäßigen Struktur des MSP-Kunden und der Topologie der Netzwerke können die folgenden typischen Konfigurationen für die Struktur der Administrationsgruppen unterschieden werden:

- Einzelbüro

- Mehrere kleine, eigenständige Büros

Typische Konfiguration des MSP-Kunden: Einzelbüro

In einer typischen Einzelbüro-Konfiguration befinden sich alle Geräte im Netzwerk des Unternehmens und können einander "sehen". Das Netzwerk des Unternehmens kann aus mehreren ausgewählten Teilen (der Netzwerke oder der Netzwerksegmente) bestehen, die über enge Kanäle verbunden sind.

Es sind die folgenden Methoden für den Aufbau der Struktur der Administrationsgruppen möglich:

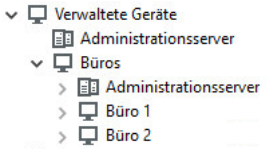
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen. Die Verteilungspunkte können automatisch bestimmt oder manuell zugewiesen werden.

- Aufbau der Struktur der Administrationsgruppen, in der die Netztopologie nicht widergespiegelt wird. In diesem Fall müssen Sie die automatische Bestimmung der Verteilungspunkte deaktivieren und dann für die Stammadministrationsgruppe in jedem ausgewählten Teil des Netzwerkes ein oder mehrere Geräte als Verteilungspunkte bestimmen, beispielsweise für die Gruppe **Verwaltete Geräte**. Alle Verteilungspunkte befinden sich dann auf einer Ebene und haben den identischen Gültigkeitsbereich, der alle Geräte im Netzwerk des Unternehmens umfasst. Jeder der Administrationsagenten wird in diesem Fall mit dem Verteilungspunkt verbunden, zu dem die Route am kürzesten ist. Die Route zum Verteilungspunkt kann mithilfe des Tools "tracert" bestimmt werden.

Typische Konfiguration des MSP-Kunden: Mehrere kleine, eigenständige Büros

Diese typische Konfiguration entspricht einigen kleinen Remote-Büros, die beispielsweise über das Internet mit dem Hauptbüro verbunden sind. Jedes der Remote-Büros befindet sich hinter einer NAT. Das bedeutet, dass ein Remote-Büro nicht mit einem anderen verbunden werden kann und die Büros voneinander isoliert sind.

Diese Konfiguration muss in der Struktur der Administrationsgruppen widergespiegelt werden: für jedes Remote-Büro muss eine separate Administrationsgruppe erstellt werden (entspr. Gruppen **Büro 1**, **Büro 2** auf der nachfolgenden Abbildung).



Die Remote-Büros werden in der Struktur der Administrationsgruppen abgebildet.

Für jede Administrationsgruppe, die einem Büro entspricht, müssen ein oder mehrere Verteilungspunkte festgelegt werden. Als Verteilungspunkte müssen Geräte des Remote-Büros bestimmt werden, die genug freien Platz auf dem Datenträger haben. Die Geräte, die sich beispielsweise in der Gruppe **Büro 1** befinden, wenden sich an die Verteilungspunkte, die für die Administrationsgruppe **Büro 1** bestimmt wurden.

Wenn einige Benutzer samt ihren Laptops physisch zwischen Büros wechseln, müssen in jedem Remote-Büro zusätzlich zu den oben erwähnten Verteilungspunkten zwei oder mehrere Geräte ausgewählt und als Verteilungspunkte für die Administrationsgruppe der obersten Ebene bestimmt werden (Gruppe **Stammgruppe für die Büros** in der obigen Abbildung).

Beispiel: Es gibt einen Laptop, der sich in der Administrationsgruppe **Büro 1** befindet, aber physisch in ein Büro gebracht wird, das der Gruppe **Büro 2** entspricht. Nach dem Ortswechsel versucht der Administrationsagent auf dem Laptop, sich an die Verteilungspunkte zu wenden, die zur Gruppe **Büro 1** gehören. Diese Verteilungspunkte erweisen sich allerdings als nicht verfügbar. Dann beginnt der Administrationsagent, sich an die Verteilungspunkte zu wenden, die für die Gruppe **Stammgruppe für die Büros** bestimmt wurden. Da die Remote-Büros voneinander isoliert sind, werden von allen Verteilungspunkten, die für die Administrationsgruppe **Stammgruppe für die Büros** bestimmt wurden, nur die Zugriffe des Administrationsagenten auf die Verteilungspunkte erfolgreich sein, die für die Gruppe **Büro 2** bestimmt wurden. Das bedeutet, dass der Laptop zwar in der Administrationsgruppe bleibt, die dem ursprünglichen Büro entspricht, aber die Verteilungspunkte jenes Büros verwendet, in dem er sich in diesen Moment physisch befindet.

Richtlinienhierarchie, Verwendung von Richtlinienprofilen

Dieser Abschnitt enthält Informationen über Besonderheiten der Anwendung von Richtlinien auf Geräte in Administrationsgruppen. Dieser Abschnitt enthält auch Informationen zu Richtlinienprofilen.

Hierarchie der Richtlinien

In Kaspersky Security Center sind Richtlinien für die Angabe eines identischen Satzes von Einstellungen auf mehreren Geräten vorgesehen. Beispielsweise betrifft der Gültigkeitsbereich der Richtlinie des Programms P, die für die Administrationsgruppe G bestimmt ist, die verwalteten Geräte mit dem installierten Programm P in der Administrationsgruppe G und allen ihren Untergruppen, mit Ausnahme jener Untergruppen, in deren Eigenschaften das Kontrollkästchen **Aus übergeordneter Gruppe erben** deaktiviert ist.

Eine Richtlinie unterscheidet sich von den lokalen Einstellungen durch das Vorhandensein von Schloss-Symbolen ( ) neben den in ihr enthaltenen Einstellungen. Ein aktiviertes "Schloss" in den Richtlinieneigenschaften bedeutet, dass die entsprechende Einstellung (bzw. die Einstellungsgruppe) erstens beim Erstellen der wirksamen Einstellungen verwendet werden soll, und zweitens auf die niedrigere Richtlinie angewendet werden soll.

Das Erstellen der auf dem Gerät geltenden Einstellungen kann auf folgende Weise realisiert werden: Aus der Richtlinie die Werte der Einstellungen mit nicht aktiviertem Schloss übernehmen und die Werte der lokalen Einstellungen darüber speichern. Dann werden über die erhaltenen Werte die aus der Richtlinie übernommenen Werte der Einstellungen mit aktiviertem Schloss gespeichert.

Die Richtlinien ein und desselben Programms beeinflussen einander gegenseitig gemäß der Hierarchie der Administrationsgruppen: die Einstellungen mit dem aktivierten Schloss aus der höher liegenden Richtlinien überschreiben die gleichnamigen Einstellungen aus der niedriger liegenden Richtlinie.

Es existiert eine besondere Art von Richtlinie, nämlich die Richtlinie für mobile Benutzer. Diese Richtlinie tritt auf einem Gerät in Kraft, wenn das Gerät in den Modus für mobile Benutzer wechselt. Mobile Richtlinien gelten gemäß der Hierarchie der Administrationsgruppen nicht auf andere Richtlinien.

Richtlinienprofile

Die Anwendung der Richtlinien auf den Geräten nur aufgrund der Hierarchie der Administrationsgruppen ist in vielen Fällen ungeeignet. Es kann erforderlich werden, in verschiedenen Administrationsgruppen mehrere Kopien einer Richtlinie zu erstellen, die sich ein bis zwei Einstellungen unterscheiden, und im Folgenden den Inhalt dieser Richtlinien manuell zu synchronisieren.

Um Ihnen zu helfen, solche Probleme zu vermeiden, unterstützt Kaspersky Security Center *Richtlinienprofile*. Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von "zugrundeliegenden" Richtlinie unterscheiden, die auf dem Client-Gerät (Computer, mobiles Gerät) gilt. Bei der Aktivierung des Profils werden die Einstellungen der bis zur Aktivierung des Profils auf dem Gerät geltenden Richtlinie geändert. Diese Einstellungen nehmen die im Profil festgelegten Werte an.

Richtlinienprofile haben derzeit folgende Einschränkungen:

- Die Richtlinie darf nicht mehr als 100 Profile enthalten.
- Ein Richtlinienprofil kann keine anderen Profile enthalten.
- Ein Richtlinienprofil darf keine Benachrichtigungseinstellungen enthalten.

Zusammensetzung des Profils

Ein Richtlinienprofil enthält die folgenden Bestandteile:

- Name. Profile mit identischen Namen wirken sich auf einander gemäß der Hierarchie der Administrationsgruppen mit den allgemeinen Regeln aus.
- Teilmenge der Richtlinieneinstellungen. Im Unterschied zur Richtlinie, in der alle Einstellungen enthalten sind, enthält ein Profil nur jene Einstellungen, die wirklich erforderlich sind (für die ein Schloss definiert ist).

- Die Aktivierungsbedingung ist ein logischer Ausdruck über den Eigenschaften des Geräts. Das Profil ist nur aktiv (ergänzt die Richtlinie), wenn die Aktivierungsbedingung des Profils erfüllt ist. In den übrigen Fällen ist das Profil inaktiv und wird ignoriert. Am logischen Ausdruck können die folgenden Geräteigenschaften teilnehmen:
  - Status des Modus für mobile Benutzer.
  - Die Eigenschaften der Netzwerkumgebung – der Name der aktiven Regel zur Verbindung des Administrationsagenten.
  - Vorhandensein oder Abwesenheit der angegebenen Tags auf dem Gerät.
  - Der Standort des Geräts im Active Directory-Einheit: explizit (das Gerät befindet sich unmittelbar in der angegebenen Organisationseinheit) oder implizit (das Gerät befindet sich in einer Organisationseinheit, die sich auf einer beliebigen Verschachtelungsebene innerhalb der angegebenen Organisationseinheit befindet).
  - Zugehörigkeit des Geräts zur Sicherheitsgruppe Active Directory (explizit oder implizit).
  - Zugehörigkeit des Gerätebesitzers zur Sicherheitsgruppe Active Directory (explizit oder implizit).
- Kontrollkästchen zum Deaktivierens des Profils. Deaktivierten Profile werden immer ignoriert, ihre Aktivierungsbedingungen werden nicht auf den Wahrheitsgehalt geprüft.
- Priorität des Profils. Die Aktivierungsbedingungen der Profile sind unabhängig, deshalb können mehrere Profile sofort gleichzeitig aktiviert werden. Wenn sich die aktiven Profile Einstellungssätze enthalten, die sich überschneiden, entstehen keine Probleme. Wenn jedoch zwei aktive Profile verschiedene Werte für ein und dieselbe Einstellung enthalten, entsteht eine Mehrdeutigkeit. Diese Mehrdeutigkeit wird mithilfe der Prioritäten der Profile entfernt: der Wert für die mehrdeutigen Variablen dem Profil mit der höheren Priorität (jenem Profil, das sich weiter oben in der Liste der Profile befindet) entnommen.

Verhalten der Profile bei der gegenseitigen Aktion der Richtlinien gemäß der Hierarchie

Gleichnamige Profile werden gemäß den Regeln zur Vereinigung von Richtlinien zusammengeführt. Profile der oberen Richtlinie haben gegenüber den Profilen der unteren Richtlinie Priorität. Wenn in "oberen" Richtlinie eine Änderung der Einstellungen verboten ist (die Schaltfläche Schloss wurde geklickt), werden in der "unteren" Richtlinie Aktivierungsbedingungen des Profils aus der "oberen" Richtlinie verwendet. Wenn in der "oberen" Richtlinie die Änderung der Einstellungen erlaubt ist, werden die Aktivierungsbedingungen des Profils aus der "unteren" Richtlinie verwendet.

Da das Richtlinienprofil in den Aktivierungsbedingungen die Eigenschaft **Gerät im autonomen Modus** enthalten kann, wird die Funktionalität der Richtlinien für mobile Benutzer vollständig durch die Profile ersetzt und nicht länger unterstützt.

Die Richtlinie für eigenständige Benutzer kann Profile enthalten, deren Aktivierung jedoch erst erfolgen kann, wenn das Gerät in den Modus für mobile Benutzer wechselt.

Aufgaben

Kaspersky Security Center verwaltet die auf Geräten installierten Sicherheitsanwendungen von Kaspersky durch das Erstellen und Starten von *Aufgaben*. Die Aufgaben ermöglichen Installation, Start und Beenden von Anwendungen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Anwendungsmodule sowie Ausführung anderer Aktionen mit den Anwendungen.

Aufgaben für eine bestimmte Anwendung können nur erstellt werden, sofern das Verwaltungs-Plug-in für diese Anwendung installiert ist.

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Die folgenden Aufgaben werden auf dem Administrationsserver ausgeführt:

- Berichte automatisch versenden
- Updates in die Datenverwaltung des Administrationsservers herunterladen
- Backup der Daten des Administrationsservers anlegen
- Datenbank bedienen
- Windows-Updates synchronisieren
- Installationspaket anhand des Betriebssystem-Abbilds eines Mustergeräts erstellen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

- *Lokale Aufgaben* sind Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

  Lokale Aufgaben können nicht nur vom Administrator mithilfe der Verwaltungskonsole geändert werden, sondern auch vom Benutzer des Remote-Geräts (beispielsweise in der Benutzeroberfläche der Sicherheitsanwendung). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

- *Gruppenaufgaben* sind Aufgaben, die auf allen Geräten einer bestimmten Gruppe ausgeführt werden.

  Soweit in den Aufgabeneigenschaften nicht anders festgelegt, betrifft eine Gruppenaufgabe auch alle Untergruppen der ausgewählten Gruppe. Eine Gruppenaufgabe betrifft (optional) auch Geräte, die mit den sekundären und virtuellen Administrationsservern in der Gruppe und den Untergruppen verbunden sind.

- *Globale Aufgaben* sind Aufgaben, die auf einem Satz von Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Gruppe gehören.

Sie können für jede Anwendung eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt von Aufgaben verfolgen, und Aufgaben kopieren, exportieren, importieren und löschen.

Eine Aufgabe wird auf einem Gerät nur dann gestartet, wenn das Programm gestartet wurde, für das diese Aufgaben erstellt worden waren.

Ergebnisse von Aufgaben werden Microsoft Windows Ereignisprotokoll und im Ereignisprotokoll von Kaspersky Security Center sowohl zentral auf dem Administrationsserver als auch lokal auf jedem Gerät gespeichert.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Verschiebungsregeln für Geräte

Das Verteilen von Geräten auf Administrationsgruppen auf einem virtuellen Server, der dem MSP-Kunden entspricht, wird sinnvollerweise mithilfe der *Regeln für das Verschieben von Geräten* automatisiert. Die Regel zum Verschieben besteht aus drei Hauptteilen: dem Namen, der Ausführungsbedingung (logischer Ausdruck über die Attribute des Geräts) und der Zieladministrationsgruppe. Die Regel verschiebt das Gerät in die Zieladministrationsgruppe, wenn die Attribute des Geräts die Bedingung für die Regelausführung erfüllen.

Alle Regeln für das Verschieben von Geräten haben Prioritäten. Der Administrationsserver prüft die Attribute des Geräts auf Übereinstimmung mit der Bedingung für die jeweilige Regelausführung in abnehmender Priorität der Regeln. Wenn die Attribute des Geräts die Bedingungen für die Regelausführung erfüllen, wird das Gerät in die Zielgruppe verschoben und beendet daraufhin die Verarbeitung der Regeln für das betreffende Gerät. Wenn die Attribute des Geräts sofort einigen Regeln entsprechen, wird das Gerät in die Zielgruppe jener Regel verschoben, welche die höchste Priorität hat (in der Liste der Regeln weiter oben steht).

Die zum Geräte verschieben können implizit erstellt werden. Beispielsweise kann in den Eigenschaften des Installationspakets oder der Aufgabe zur Remote-Installation die Administrationsgruppe angegeben werden, in die das Gerät gelangen soll, nachdem darauf der Administrationsagent installiert wurde. Darüber hinaus können die Regeln zum Verschieben vom Administrator von Kaspersky Security Center auf offensichtliche Art in der Liste der Regeln zum Verschieben erstellt werden. Die Liste befindet sich in der Verwaltungskonsole in den Eigenschaften der Gruppe **Nicht zugeordnete Geräte**.

Die Regel zum Verschiebung ist standardmäßig für die einmalige erstmalige Verteilung der Geräte auf die Administrationsgruppen vorgesehen. Die Regel verschiebt die Geräte, die sich in der Gruppe **Nicht zugeordnete Geräte** befinden, nur einmal. Wenn ein Gerät von dieser Regel einmal verschoben wurde, wird es nicht nochmals von der Regel verschoben, selbst wenn das Gerät manuell erneut in die Gruppe **Nicht zugeordnete Geräte** verschoben wird. Dies ist die empfohlene Art der Nutzung der Regeln zum Verschieben.

Es können Geräte verschoben werden, die sich bereits in Administrationsgruppen befinden. Dazu muss in den Eigenschaften der Regel das Kontrollkästchen **Nur Geräte verschieben, die sich nicht in den Administrationsgruppen befinden** deaktiviert werden.

Durch die Existenz von Regeln zum Verschieben, die auf Geräte gelten, die bereits in die Administrationsgruppen verschoben wurden, steigt die Belastung auf dem Administrationsserver erheblich.

Es kann eine Regel zum Verschieben erstellt werden, die auf einem Gerät mehrfach ausgeführt werden kann.

Es wird dringend empfohlen, Szenarien zu vermeiden, bei denen ein verwaltetes Gerät mehrfach aus einer Gruppe in eine andere verschoben wird (z. B. um eine besondere Richtlinie auf das Gerät anzuwenden, eine spezielle Gruppenaufgabe zu starten oder das Gerät über einen bestimmten Verteilungspunkt zu aktualisieren).

Solche Szenarien werden nicht unterstützt, da sie die Belastung des Administrationsservers und den Datenverkehr in extremem Ausmaß erhöhen. Diese Szenarien stehen ferner in Konflikt mit den Betriebsprinzipien von Kaspersky Security Center (insbesondere im Bereich von Zugriffsrechen, Ereignissen und Berichten). Es müssen andere Lösungen gesucht werden, zum Beispiel durch Verwendung der Richtlinienprofile, der Aufgaben für Geräteauswahlen, die Zuweisung von Administrationsagenten entsprechend dem Standardszenario und so weiter.

Software-Kategorisierung

Das wichtigste Tool zur Kontrolle des Starts von Apps sind die *Kategorien von Kaspersky* (im Weiteren auch *KL-Kategorien*). Die KL-Kategorien erleichtern dem Administrator von Kaspersky Security Center die Aufrechterhaltung der Kategorisierung der Software und verringern den Umfang des Datenverkehrs, der an die verwalteten Geräte übergeben wird.

Benutzerdefinierte Kategorien müssen nur für Programme erstellt werden, die nicht unter eine KL-Kategorie fallen (beispielsweise für Programme, die auf Bestellung entwickelt wurden). Die benutzerdefinierten Kategorien werden auf der Grundlage der Programmpakete (MSI) oder auf der Grundlage des Ordners mit den Installationspaketen erstellt.

Falls es eine umfangreiche ergänzte Software-Sammlung gibt, die mithilfe der KL-Kategorien kategorisiert ist, kann es zweckmäßig sein, eine automatisch aktualisierte Kategorie zu erstellen. Eine solche Kategorie wird bei der Änderung des Ordners mit den Programmpaketen automatisch mit den Prüfsummen der ausführbaren Dateien ergänzt.

Erstellen Sie keine automatisch aktualisierten Programmkategorien für die folgenden Ordner: "Eigene Dateien", "%windir%', '%Programme%" und %Programme (x86)%. Die Dateien in diesen Ordnern ändern sich oft, was zur Erhöhung der Belastung auf den Administrationsserver und zur Erhöhung des Datenverkehres im Netzwerk führt. Es muss ein separater Ordner mit der Sammlung der Software erstellt und von Zeit zu Zeit ergänzt werden.

Mandantenfähige Programme

Kaspersky Security Center ermöglicht Administratoren von Dienstanbietern und Mandantenadministratoren die Verwendung von Kaspersky-Anwendungen mit Unterstützung der Mandantenfähigkeit. Nach der Installation einer mandantenfähigen Kaspersky-Anwendung in der Infrastruktur des Dienstanbieters können Mandanten mit der Verwendung des Programms beginnen.

Um die Aufgaben und Richtlinien verschiedener Mandanten voneinander abzuschotten, muss für jeden Mandanten ein dedizierter virtueller Administrationsserver in Kaspersky Security Center erstellt werden. Alle Aufgaben und Richtlinien für mandantenfähige Programme, die für einen Mandanten ausgeführt werden, müssen für die Administrationsgruppe "Verwaltete Geräte" des virtuellen Administrationsservers des entsprechenden Mandanten erstellt werden. Die Aufgaben, die für die Administrationsgruppen des primären Administrationsservers erstellt werden, haben keine Auswirkung auf die Geräte der Mandanten.

Im Unterschied zu Administratoren von Dienstanbietern kann ein Mandantenadministrator nur für die Geräte des entsprechenden Mandanten Aufgaben und Programmrichtlinien erstellen und ansehen. Administratoren von Dienstanbietern und Mandantenadministratoren steht jeweils eine andere Auswahl an Aufgaben und Richtlinieneinstellungen zur Verfügung. Einige der Aufgaben und Richtlinieneinstellungen sind nicht für Mandantenadministratoren verfügbar.

Innerhalb der Hierarchiestruktur eines Mandanten werden die für mandantenfähige Programme erstellten Richtlinien an untergeordnete und übergeordnete Administrationsgruppen vererbt: Die Richtlinie wird an alle Client-Geräte verteilt, die zum Mandanten gehören.

Verschieben ins Backup und Wiederherstellen der Einstellungen des Administrationsservers

Für das Verschieben der Einstellungen des Administrationsservers und der von ihm verwendeten Datenbank ins Backup ist die Aufgabe zum Verschieben ins Backup und das Tool klbackup vorgesehen. Die Backup-Kopie umfasst alle Haupteinstellungen und Objekte des Administrationsservers: die Zertifikate des Administrationsservers, die Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte, die Lizenzschlüssel, die Struktur der Administrationsgruppen mit sämtlichem Inhalt, die Aufgaben, die Richtlinien und mehr. Mit einer Backup-Kopie kann die Funktionsfähigkeit eines Administrationsservers schnellstmöglich wiederhergestellt werden, was wenige Minuten oder bis zu zwei Stunden dauern kann.

Bei einer fehlenden Backup-Kopie kann eine Störung zum unwiederbringlichen Verlust der Zertifikate und aller Einstellungen des Administrationsservers führen. Kaspersky Security Center muss dann erneut konfiguriert werden und die erstmalige Bereitstellung des Administrationsagenten im Netzwerk des Unternehmens muss erneut ausgeführt werden. Außerdem gehen auch alle Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte verloren, was das Risiko eines unwiederbringlichen Verlustes der verschlüsselten Daten auf den Geräten mit Kaspersky Endpoint Security mit sich bringt. Auf das regelmäßige Erstellen von Backup-Kopien des Administrationsservers mithilfe der Standardaufgabe zum Verschieben ins Backup darf keinesfalls verzichtet werden.

Der Schnellstartassistent erstellt die Aufgabe zum Anlegen eines Backups der Einstellungen des Administrationsservers mit einem täglichen Start um 4:00 Uhr morgens. Gespeichert werden die Backup-Kopien standardmäßig im Ordner %ALLUSERSPROFILE%\Application Data\KasperskySC.

Wenn als DBMS ein Instanz von Microsoft SQL Server, die auf einem anderen Gerät installiert ist, verwendet wird, muss die Aufgabe zum Verschieben ins Backup geändert werden: als Ordner für die Speicherung der erstellten Backup-Kopien muss der UNC-Pfad angegeben werden, der sowohl als Dienst des Administrationsservers als auch als Dienst für SQL Server für einen Eintrag verfügbar ist. Diese Anforderung ist eine Folge der Untersuchung des Verschiebens ins Backup im DBMS Microsoft SQL Server.

Wenn als DBMS eine lokale Instanz von Microsoft SQL Server verwendet wird, empfehlen wir außerdem, die Backup-Kopien auf einem separaten Datenträger zu speichern, um sie gleichzeitig mit dem Administrationsserver vor Beschädigung zu sichern.

Da eine Backup-Kopie wichtige Daten enthält, ist in der Aufgabe zum Verschieben ins Backup und im Tool klbackup der Schutz der Backup-Kopien durch ein Kennwort vorgesehen. Standardmäßig wird die Aufgabe zum Verschieben ins Backup mit einem leeren Kennwort erstellt. Das Kennwort muss in den Eigenschaften der Aufgabe zum Verschieben ins Backup unbedingt festgelegt werden. Wenn diese Forderung nicht erfüllt wird, führt das dazu, dass die Schlüssel der Zertifikate des Administrationsservers, die Schlüssel für die Lizenzen und die Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte nicht verschlüsselt sind.

Neben dem regelmäßigen Verschieben ins Backup muss auch eine Backup-Kopie aller wichtiger Änderungen erstellt werden, darunter auch vor dem Update des Administrationsservers auf die neue Version und vor der Installation der Patches des Administrationsservers.

Wenn Sie Microsoft SQL Server als DBMS verwenden, können Sie die Größe der Sicherungskopien minimieren. Um dies zu tun, aktivieren Sie das Kontrollkästchen **Backup komprimieren** (Compress backup) in den SQL Server-Einstellungen.

Die Wiederherstellung aus der Backup-Kopie wird mithilfe des Tools klbackup mit der gerade erst installierten und funktionsfähigen Instanz des Administrationsservers jener Version durchgeführt, für die eine Backup-Kopie erstellt wurde (oder neuer).

Die Instanz des Administrationsservers, auf der die Wiederherstellung ausgeführt werden soll, muss ein DBMS desselben Typs (z. B. der gleiche SQL Server oder MariaDB) und derselben Version oder höher verwenden. Die Version des Administrationsservers kann gleich (mit einem ähnlichen oder neueren Patch) oder neuer sein.

In diesem Abschnitt werden typische Szenarien für die Wiederherstellung der Einstellungen und der Objekte des Administrationsservers beschrieben.

Ein Gerät mit dem Administrationsserver ist ausgefallen

Wenn das Gerät mit dem Administrationsserver infolge einer Störung außer Betrieb ist, wird empfohlen, wie folgt vorzugehen:

- Dem neuen Administrationsserver dieselbe Adresse zuweisen: NetBIOS-Name, FQDN-Name, statische IP-Adresse, wobei berücksichtigt werden muss, was bei der Bereitstellung des Administrationsagenten festgelegt wurde.

- Administrationsserver unter Verwendung eines DBMS desselben Typs und derselben oder einer neueren Version installieren. Es kann dieselbe Version des Servers mit demselben oder einem neueren Patch, oder eine neuere Version installiert werden. Nach der Installation muss keine Erstkonfiguration mithilfe des Assistenten ausgeführt werden.

- Starten Sie im Menü **Start** das Tool "klbackup" und führen Sie die Wiederherstellung durch.

Die Einstellungen des Administrationsservers oder der Datenbank sind beschädigt

Wenn der Administrationsserver infolge der Beschädigung der Einstellungen oder der Datenbank funktionsunfähig wurde (beispielsweise wegen eines Stromausfalls), wird empfohlen, das folgende Szenario für die Wiederherstellung zu verwenden:

1. Untersuchung des Dateisystems auf dem betroffenen Gerät durchführen.
2. Funktionsunfähige Version des Administrationsservers deinstallieren.
3. Administrationsserver unter Verwendung eines DBMS desselben Typs und derselben oder einer neueren Version erneut installieren. Es kann dieselbe Version des Servers mit demselben oder einem neueren Patch, oder eine neuere Version installiert werden. Nach der Installation muss keine Erstkonfiguration mithilfe des Assistenten ausgeführt werden.
4. Das Sicherungs- u. Wiederherstellungstool klbackup aus dem Menü **Start** ausführen und die Wiederherstellung ausführen.

Es ist unmöglich, den Administrationsserver auf andere Weise als mit dem Standardtool klbackup wiederherzustellen.

In sämtlichen Fälle der Wiederherstellung des Administrationsservers mithilfe von Drittanbieter-Programmen kommt es unvermeidlich zu einer Desynchronisierung der Daten in den Knoten des verteilten Programms Kaspersky Security Center und in der Folge zu einer inkorrekten Ausführung des Programms.

Softwareverteilung für den Administrationsagenten und die Sicherheitsanwendung

Zur Verwaltung der Unternehmensgeräte muss auf den Geräten der Administrationsagent installiert werden. Die Bereitstellung der verteilten App Kaspersky Security Center auf den Geräten des Unternehmens beginnt gewöhnlich mit der Installation des Administrationsagenten.

Unter Windows XP führt der Administrationsagent folgende Operationen möglicherweise nicht korrekt aus: Das Herunterladen von Updates direkt von den Servern von Kaspersky (als Verteilungspunkt), das Fungieren als KSN-Proxyserver (als Verteilungspunkt) und das Erkennen von Schwachstellen bei Drittanbietern (wenn die Funktion Schwachstellen- und Patch-Management genutzt wird).

Erstmalige Bereitstellung

Wenn auf einem Gerät der Administrationsagent schon installiert ist, erfolgt die Remote-Installation der Apps auf einem solchen Gerät mithilfe des Administrationsagenten. Dabei wird die Übertragung des Programmpakets der zu installierenden App zusammen mit den vom Administrator festgelegten Installationseinstellungen über die Verbindungskanäle zwischen den Administrationsagenten und dem Administrationsserver durchgeführt. Für die Übertragung des Programmpakets können Sie Knoten zur weiteren Verteilung in Form von Verteilungspunkten, Multicast-Versand usw. verwendet werden. Ausführliche Information über die Installation von Apps auf den verwalteten Geräten, auf denen der Administrationsagent schon installiert ist, finden Sie später in diesem Abschnitt.

Die erstmalige Installation des Administrationsagenten auf den Geräten auf der Microsoft Windows-Plattform kann auf folgende Arten erfolgen:

- Mithilfe von Dritthersteller-Tools zur Remote-Installation von Apps.
- Mithilfe des Mechanismus der Microsoft Windows-Gruppenrichtlinien: mithilfe der Standardtools zur Verwaltung von Microsoft Windows-Gruppenrichtlinien.
- Erzwungen mithilfe der entsprechenden Optionen in der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center.
- Mittels Versand eines Links auf die von Kaspersky Security Center gebildeten autonomen Pakete an die Benutzer der Geräte. Die autonomen Pakete stellen ausführbare Module dar, in denen die Programmpakete der ausgewählten Programme mit den konfigurierten Einstellungen enthalten sind.
- Manuell durch Starten der Installer der Programme auf den Geräten.

Auf anderen Plattformen als Microsoft Windows muss die erstmalige Installation des Administrationsagenten auf den verwalteten Geräten entweder mithilfe der vorhandenen Drittanbieter-Tools oder manuell erfolgen, indem das Archiv mit dem vorkonfigurierten Programmpaket an die Benutzer gesendet wird. Mithilfe der Aufgaben zur Remote-Installation von Anwendungen und unter Verwendung von schon auf den Geräten vorhandenen Administrationsagenten können der Administrationsagent auf die neue Version aktualisiert und andere Kaspersky-Anwendungen auf diesen Plattformen installiert werden. Die Installation erfolgt in diesem Fall analog zur Installation auf Geräten mit Microsoft Windows.

Bei der Auswahl von Methode und Strategie zur Bereitstellung der Programme im verwalteten Netzwerk muss eine Reihe von Faktoren beachtet werden (unvollständige Liste):

- Konfiguration des Unternehmensnetzwerks
- Gesamtzahl der Geräte
- Vorhandensein von Windows-Domänen im verwalteten Netzwerk, Möglichkeit der Bearbeitung der Gruppenrichtlinien des Active Directory in solchen Domänen
- Kenntnis des Benutzerkontos bzw. der Konten mit den Rechten des lokalen Administrators auf jenen Geräten, auf denen die erste Bereitstellung der Kaspersky-Anwendungen vorgenommen werden soll (d. h. die Verfügbarkeit eines Domänen-Benutzerkontos mit den Rechten des lokalen Administrators oder das Vorhandensein von einheitlichen lokalen Benutzerkonten mit Verwaltungsrechten auf solchen Geräten)

- Art der Verbindung und Bandbreite der Netzwerkkanäle zwischen dem Administrationsserver und den Netzwerken der MSP-Kunden sowie die Bandbreite der Netzwerkkanäle innerhalb jener Netzwerke

- Zum Startzeitpunkt der Bereitstellung verwendete Sicherheitseinstellungen auf den Remote-Geräten (insbesondere Nutzung von UAC und des Modus Simple File Sharing)

Anpassen der Einstellungen der Installer

Vor Beginn der Bereitstellung der Kaspersky-Anwendungen im Netzwerk müssen die Installationseinstellungen festgelegt werden – jene Einstellungen bestimmen, die im Verlauf der Programminstallation angepasst werden. Bei der Installation des Administrationsagenten müssen zumindest die Adresse für die Verbindung mit dem Administrationsserver, die Proxy-Einstellungen und nach Möglichkeit auch einige erweiterte Einstellungen festgelegt werden. Abhängig von der ausgewählten Installationsmethode können die Einstellungen auf verschiedenen Weisen festgelegt werden. Im einfachsten Fall (bei der interaktiven manuellen Installation auf dem ausgewählten Gerät) können die erforderlichen Einstellungen über die Benutzeroberfläche des Installers angegeben werden, d. h. in einigen Fällen kann die erstmalige Bereitstellung vorgenommen werden, indem den Benutzern Links zum Programmpaket des Administrationsagenten mit Angabe der Einstellungen (Adresse des Administrationsservers u. ä.) gesendet wird, die der Benutzer in der Benutzeroberfläche des Installers eingibt.

In der Praxis wird diese Konfigurationsmethode nicht empfohlen, da sie umständlich für Benutzer ist und da die manuelle Eingabe von Einstellungen fehleranfällig ist. Zudem eignet sie sich nicht zur Silent-Installation von Programmen auf einer Gruppe von Geräten. Im Normalfall muss der Administrator die Einstellungswerte, die im Weiteren für die Erstellung von autonomen Paketen verwendet werden können, zentralisiert angeben. Autonome Pakete sind selbst entpackende Archive der Programmpakete mit vom Administrator festgelegten Einstellungen. Autonome Pakete können sich auf Ressourcen befinden, auf denen sie für den Download durch Endbenutzer (z. B. auf dem Kaspersky Security Center Webserver) und für eine Silent-Installation auf den ausgewählten Geräten im Netzwerk verfügbar sind.

Installationspakete

Die erste und wichtigste Methode zur Konfiguration der Installationseinstellungen der Apps ist universell und kommt für alle Installationsmethoden der Apps in Frage: sowohl mithilfe von Kaspersky Security Center als auch mithilfe der meisten Drittanbieter-Tools. Diese Methode bedingt das Erstellen der Installationspakete der Apps in Kaspersky Security Center.

Die Installationspakete werden auf folgende Arten erstellt:

- Automatisch aus den angegebenen Programmpaketen auf der Grundlage *Beschreibungen* in ihren Bestand (Dateien mit der Erweiterung kud, die Regeln für Installation und Analyse des Ergebnisses und andere Informationen enthalten)

- Aus den ausführbaren Dateien der Installer oder der Installer im Format Microsoft Windows Installer (MSI), für Standard-Apps oder unterstützte Apps

Die erstellten Installationspakete bestehen aus einer Hierarchie von Ordnern mit Unterordnern und Dateien. Neben den originalen Programmpaketen umfasst das Installationspaket die bearbeiteten Einstellungen (einschließlich der Einstellungen des Installers und der Regel zur Verarbeitung von Situationen wie ein erforderlicher für den Abschluss der Installation Neustart des Betriebssystems), sowie kleine Hilfsmodule.

Die Werte der Installationseinstellungen, die für die konkrete unterstützte Anwendung spezifisch sind, können in der Benutzeroberfläche der Verwaltungskonsole bei der Erstellung des Installationspakets angegeben werden (weitere Einstellungen sind in den Eigenschaften des bereits erstellten Installationspakets verfügbar). Im Fall einer Remote-Installation der Programme mithilfe von Kaspersky Security Center werden die Installationspakete so an die Geräte geliefert, dass beim Start des Installers des Programms alle vom Administrator festgelegten Einstellungen verfügbar sind. Bei Verwendung von Drittanbieter-Tools zur Installation der Kaspersky-Anwendungen ist es ausreichend, die Verfügbarkeit des gesamten Installationspakets, das heißt des Programmpakets und dessen Einstellungen, auf dem Gerät zu gewährleisten. Die Installationspakete werden erstellt und von Kaspersky Security Center in einem entsprechenden Unterordner des gemeinsamen Verzeichnisses aufbewahrt.

Geben Sie in den Einstellungen der Installationspakete keine Daten von privilegierten Benutzerkonten an.

Anweisungen zur Verwendung dieser Konfigurationsmethode für Kaspersky-Anwendungen vor der Bereitstellung durch Drittanbieter-Tools finden Sie im Abschnitt Bereitstellung mithilfe des Mechanismus der Gruppenrichtlinien von Microsoft Windows.

Sofort nach der Installation von Kaspersky Security Center werden automatisch mehrere Installationspakete erstellt, die bereit zur Installation sind, darunter die Pakete des Administrationsagenten und der Sicherheitsanwendungen für die Plattform Microsoft Windows.

Die Verwendung von Installationspaketen für die Bereitstellung im Netzwerk des MSP-Kunden setzt in bestimmten Fällen voraus, dass Installationspakete auf virtuellen Servern, die den MSP-Kunden entsprechen, erstellt werden. Die Erstellung von Installationspaketen auf virtuellen Servern ermöglicht die Verwendung von verschiedenen Installationseinstellungen in den Installationspaketen für verschiedene MSP-Kunden. In erster Linie wird dies für Installationspakete des Administrationsagenten benötigt, da die Administrationsagenten, die in den Netzwerken verschiedener MSP-Kunden bereitgestellt wurden, verschiedene Adressen für die Verbindung mit dem Administrationsserver verwenden. Die Adresse für die Verbindung bestimmt letztendlich auch, mit welchem virtuellen Server der Administrationsagent verbunden wird.

Neben der Möglichkeit, neue Installationspakete direkt auf dem virtuellen Administrationsserver zu erstellen, gehört die Verteilung von Installationspaketen vom primären Administrationsserver auf die virtuellen Administrationsserver zum Hauptaspekt der Verwendung von Installationspaketen auf virtuellen Servern. Die ausgewählten (oder alle) Installationspakete können mithilfe der entsprechenden Aufgabe des Administrationsservers auf die ausgewählten virtuellen Administrationsserver (einschließlich aller Server, die zur entsprechenden Administrationsgruppe gehören) verteilt werden. Darüber hinaus kann bei der Erstellung eines neuen virtuellen Administrationsservers im Assistenten eine Liste mit Installationspaketen des primären Administrationsservers ausgewählt werden. Die ausgewählten Pakete werden sofort auf dem neu erstellten virtuellen Administrationsserver verteilt.

Bei der Verteilung des Installationspakets wird sein Inhalt nicht vollständig kopiert. In der Datenverwaltung, die dem verteilten Installationspaket auf dem virtuellen Administrationsserver entspricht, werden nur die Dateien der Einstellungen gespeichert, die für den jeweiligen virtuellen Server spezifisch sind. Der unveränderliche Hauptbestandteil des Installationspakets (einschließlich des Programmpakets der zu installierenden Anwendung) wird nur in der Datenverwaltung des primären Administrationsservers aufbewahrt. Dies ermöglicht eine wesentliche Steigerung der Systemleistung und eine Reduzierung des erforderlichen Speicherplatzes. Bei der Verarbeitung von Installationspaketen, die per Verteilung auf die virtuellen Administrationsserver weitergeleitet wurden (d. h. bei der Ausführung der Aufgaben zur Remote-Installation oder bei der Erstellung von autonomen Installationspaketen) erfolgt eine Zusammensetzung der Daten aus dem Ausgangsinstallationspaket des primären Administrationsservers und der Dateien mit den Einstellungen, die dem verteilten Paket auf dem virtuellen Administrationsserver entsprechen.

Obwohl es möglich ist, den Lizenzschlüssel für das Programm in den Eigenschaften des Installationspakets anzugeben, sollte diese Lizenzverteilungsmethode nicht verwendet werden, da es in diesem Fall einfach ist, versehentlich Lesezugriff auf die Dateien in diesem Ordner zu erlangen. Es wird empfohlen, automatisch verteilte Lizenzschlüssel oder Aufgaben zur Installation von Lizenzschlüsseln zu verwenden.

Eigenschaften des MSI-Installers und der Transformationsdateien

Die Anpassung der Installationseinstellungen auf der Windows-Plattform ist Aufgabe der MSI-Eigenschaften und der Transformationsdateien. Diese Methode kann bei der Installation mithilfe von Drittanbieter-Tools verwendet werden, die mit Installern im Format Microsoft Installer arbeiten. Sie kann auch bei der Installation über Windows-Gruppenrichtlinien mithilfe der Microsoft-Standardtools oder anderer Drittanbieter-Tools für die Arbeit mit Windows-Gruppenrichtlinien verwendet werden.

Bereitstellung mithilfe von Drittanbieter-Tools zur Remote-Installation von Apps

Sollten im Unternehmen irgendwelche Tools zur Remote-Installation von Apps vorhanden sein (beispielsweise Microsoft System Center), ist es sinnvoll, die erstmalige Bereitstellung mithilfe dieser Tools auszuführen.

Folgende Aktionen müssen ausgeführt werden:

- Die Konfigurationsart für die Installationseinstellungen auswählen, die sich am besten für die verwendete Methode der Bereitstellung eignet.
- Den Synchronisierungsmechanismus zwischen der Änderung der Einstellungen der Installationspakete über die Benutzeroberfläche der Verwaltungskonsole und der Arbeit der ausgewählten Drittanbieter-Tools zur Bereitstellung der Apps aus den betreffenden Installationspaketen bestimmen.

Allgemeinen Angaben über die Aufgaben zur Remote-Installation der Apps von Kaspersky Security Center

Kaspersky Security Center bietet vielfältige Mechanismen zur Remote-Installation von Anwendungen, die in Form von Aufgaben zur Remote-Installation von Anwendungen realisiert werden. Die Aufgabe zur Remote-Installation kann sowohl für die angegebene Administrationsgruppe als auch für eine Reihe von Geräten oder für Geräteauswahlen erstellt werden (diese Aufgaben werden in der Verwaltungskonsole im Ordner **Aufgaben** angezeigt). Beim Erstellen der Aufgabe können die Installationspakete (des Administrationsagenten und/oder anderer Anwendungen) ausgewählt werden, die mithilfe der betreffenden Aufgabe installiert werden, sowie eine Reihe von Einstellungen festgelegt werden, mit denen die Art der Remote-Installation bestimmt wird.

Aufgaben für Administrationsgruppen gelten nicht nur auf den Geräten, die zu dieser Gruppe gehören, sondern auch auf allen Geräte aller Untergruppen der ausgewählten Gruppe. Wenn in den Aufgabeneinstellungen die entsprechende Einstellung aktiviert ist, erstreckt sich die Aufgabe auf die Geräte der sekundären Administrationsserver, die sich in der betreffenden Gruppe oder ihren Untergruppen befinden.

Aufgaben für eine Reihe von Geräten aktualisieren die Liste der Client-Geräte bei jedem Start entsprechend der Zusammensetzung der Geräteauswahlen zum Zeitpunkt des Aufgabenstarts. Wenn sich in der Geräteauswahl Geräte befinden, die mit sekundären Administrationsservern verbunden sind, wird die Aufgabe auch auf diesen Geräten ausgeführt.

Für die erfolgreiche Ausführung der Aufgabe zur Remote-Installation auf Geräten, die mit sekundären Administrationsserver verbunden sind, müssen die von der Aufgabe verwendeten Installationspakete vorher mithilfe der Verteilungsaufgabe an die entsprechenden sekundären Administrationsserver verteilt werden.

Bereitstellung mithilfe des Mechanismus der Gruppenrichtlinien von Microsoft Windows

Es wird empfohlen, die erstmalige Bereitstellung der Administrationsagenten bei Erfüllung der folgenden Bedingungen mithilfe der Gruppenrichtlinien von Microsoft Windows zu verwirklichen:

- Das Gerät gehört zur Domäne Active Directory.
- Der Zugriff auf den Domänencontroller mit Administratorrechten ist erlaubt, was die Erstellung und Bearbeitung von Gruppenrichtlinien des Active Directory ermöglicht.
- Die Möglichkeit zur Übertragung konfigurierter Installationspakete ins Netzwerk der verwalteten Geräte (in einen freigegebenen Ordner, für den alle Geräte Leserechte besitzen) ist verfügbar.
- Der Plan zur Bereitstellung erlaubt, den standardmäßigen Neustart der Geräte abzuwarten, bevor darauf mit der Bereitstellung des Administrationsagenten begonnen wird, oder auf den Geräten kann zwangsläufig die Windows-Gruppenrichtlinie verwendet werden.

Die vorliegende Methode der Bereitstellung besteht im Wesentlichen aus Folgendem:

- Das Programmpaket im Format Microsoft Installer (MSI-Paket) wird in den freigegebenen Ordner (Ordner, für den die Benutzerkonten "LocalSystem" der Geräte Lesezugriff haben) verschoben.
- In der Gruppenrichtlinie Active Directory wird das Installationsobjekt des vorliegenden Programmpakets erstellt.

- Der Gültigkeitsbereich der Installation wird durch Anbinden an die Organisationseinheit (OU) und/oder an die Sicherheitsgruppe, zu der die Geräte gehören, angegeben.

- Bei der nächsten Anmeldung des Geräts in der Domäne (vor der Anmeldung der Benutzer des Geräts) wird geprüft, ob die erforderliche App unter den installierten Apps vorhanden ist. Wenn die App fehlt erfolgt ein Download des Programmpakets von der in der Richtlinie festgelegten Ressource und dessen Installation.

Einer der Vorteile dieser Methode der Bereitstellung ist, dass die festgelegten Apps beim Download des Betriebssystems noch vor der Anmeldung des Benutzers im System auf den Geräten installiert werden. Selbst wenn der Benutzer, der über die erforderlichen Berechtigungen verfügt, die Apps löscht, wird sie beim nächsten Download des Betriebssystems wieder installiert. Ein Nachteil dieser Methode der Bereitstellung besteht darin, dass die vom Administrator erzeugten Änderungen in der Gruppenrichtlinie bis zum Neustart der Geräte (ohne Anwendung zusätzlicher Tools) nicht in Kraft treten.

Mithilfe der Gruppenrichtlinien können sowohl der Administrationsagent als auch andere Apps installiert werden, deren Installer das Format Windows Installer haben.

> Die Installation des Administrationsagenten mittels msi-Paket ist nur im Silent-Modus möglich. Die interaktive Installation mittels msi-Paket wird nicht unterstützt.

Bei der Auswahl dieser Methode der Bereitstellung muss unter anderem die Belastung der Dateiressource berücksichtigt werden, von der das Kopieren der Dateien auf die Zielgeräte bei der Anwendung der Windows-Gruppenrichtlinie ausgeführt wird. Außerdem muss die Methode der Übertragung des konfigurierten Installationspakets (und der Synchronisierung aller in seinen Einstellungen vorgenommenen Änderungen) auf die Ressource berücksichtigt werden.

Die Arbeit mit den Microsoft Windows-Richtlinien mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center

Diese Methode der Bereitstellung ist nur möglich, wenn der Zugriff auf den Controller der Domäne, zu der die Geräte gehören, vom Gerät aus möglich ist, auf dem der Administrationsserver installiert ist, und wenn die Geräte Lesezugriff auf den freigegebenen Ordner des Administrationsservers (mit den Installationspaketen) haben. Deshalb wird diese Methode der Bereitstellung in Bezug auf MSP nicht berücksichtigt.

Selbstständige Installation von Apps mithilfe der Microsoft Windows-Richtlinien

Der Administrator kann in der Windows-Gruppenrichtlinie die für die Installation erforderlichen Objekte selbständig erstellen. In diesem Fall müssen die Pakete auf einen separaten Dateiserver übermittelt und verlinkt werden.

Es sind folgende Installationsszenarien möglich:

- Der Administrator erstellt das Installationspaket und passt dessen Eigenschaften in der Verwaltungskonsole an. Dann kopiert der Administrator den gesamten Unterordner EXEC dieses Pakets aus dem freigegebenen Ordner von Kaspersky Security Center in den Ordner auf der speziellen Dateiressource des Unternehmens. Das Gruppenrichtlinienobjekt verweist auf die msi-Datei dieses Pakets, die in einem Unterordner auf der spezialisierten Dateiressource des Unternehmens liegt.

- Der Administrator lädt das Programmpaket (einschließlich das des Administrationsagenten) aus dem Internet herunter und lädt es auf die vorgesehene Dateiressource des Unternehmens hoch. Das Gruppenrichtlinienobjekt verweist auf die msi-Datei dieses Pakets, die in einem Unterordner auf der spezialisierten Dateiressource des Unternehmens liegt. Das Anpassen der Installationseinstellungen erfolgt mittels Konfiguration der MSI-Eigenschaften oder der Konfiguration der MST-Transformationsdateien.

Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center

Um die erstmalige Bereitstellung des Administrationsagenten oder von anderen Anwendungen durchzuführen, können Sie die Installation der ausgewählten Installationspakete mithilfe der Aufgabe zur Remote-Installation von Kaspersky Security Center erzwingen. Voraussetzung dafür ist jedoch, das jedes Gerät über mindestens ein Benutzerkonto mit lokalen Administratorrechten verfügt.

Die erzwungene Installation kann auch verwendet werden, falls die Geräte nicht unmittelbar für den Administrationsserver verfügbar sind: wenn sich die Geräte beispielsweise in isolierten Netzwerken befinden oder wenn sich die Geräte im lokalen Netzwerk befinden und der Administrationsserver in der demilitarisierten Zone befindet.

Im Falle einer erstmaligen Bereitstellung ist noch kein Administrationsagent installiert. Daher können Sie in den Einstellungen der Aufgabe zur Remote-Installation nicht die Option auswählen, die zur Installation der Anwendung benötigten Dateien mithilfe des Administrationsagent zu verteilen. Sie können die Dateien lediglich unter Verwendung der Betriebssystemressourcen durch den Administrationsserver und die Verteilungspunkte verteilen.

Auf den Zielgeräten muss der Dienst des Administrationsservers unter einem Benutzerkonto mit Administratorrechten ausgeführt werden. Alternativ können Sie in den Einstellungen der Aufgabe zur Remote-Installation ein Benutzerkonto angeben, das Zugriff auf die Freigabe "admin$" hat.

> Standardmäßig verwendet die Aufgabe zur Remote-Installation zur Verbindungsherstellung mit den Geräten die Anmeldedaten des Benutzerkontos, unter dem der Administrationsserver ausgeführt wird (das Benutzerkonto mit Zugriff auf die Freigabe "admin$"). Sie müssen dieses Benutzerkonto nur dann in den Einstellungen der Aufgabe zur Remote-Installation angeben, wenn auf den Zielgeräten kein Administrationsagent installiert ist.
> Wenn Sie eine Aufgabe zur Remote-Installation erstellen, die von Linux-Geräten ausgeführt werden soll, müssen Sie immer ein Konto zum Herstellen einer SSH-Verbindung angeben.

Angeben können Sie die Geräte entweder explizit (mittels Liste), indem Sie die Administrationsgruppe von Kaspersky Security Center auswählen, in der die Geräte enthalten sind, oder durch das Erstellen einer Geräteauswahl nach bestimmten Bedingungen. Der Startzeitpunkt der Installation wird durch den Zeitplan der Aufgabe bestimmt. Wenn in den Eigenschaften der Aufgabe die Einstellung **Übersprungene Aufgaben starten** aktiviert ist, kann die Aufgabe sofort bei der Aktivierung der Geräte oder bei ihrer Übertragung in die Ziel-Administrationsgruppe ausgeführt werden.

Die erzwungene Installation erfolgt mittels Übertragung der Installationspakete an die Zielgeräte, dem anschließenden Kopieren der Dateien in die admin$-Ressource der jeweiligen Geräte und der Remote-Anmeldung der Hilfsdienste auf diesen Geräten. Die Übertragung der Installationspakete an die Zielgeräte wird mithilfe der für die Netzwerkinteraktion verantwortlichen Funktion von Kaspersky Security Center ausgeführt. Dabei müssen die folgenden Bedingungen erfüllt werden:

- Die Zielgeräte können sowohl vom Administrationsserver als auch von den Verteilungspunkten erreicht werden.
- Die Namensauflösung für die Zielgeräte funktioniert im Netzwerk fehlerfrei.
- Die freigegebenen Administratorressourcen (admin$) verbleiben auf den Zielgeräten aktiviert.
- Die folgenden Systemdienste werden auf Zielgeräten ausgeführt:
  - Server (LanmanServer)

    Dieser Dienst wird standardmäßig ausgeführt.

- DCOM Server Process Launcher (DcomLaunch)
- RPC Endpoint Mapper (RpcEptMapper)
- Remote Procedure Call (RpcSs)

- Der TCP-Port 445 ist auf den Zielgeräten geöffnet, um Remote-Zugriff mittels Windows-Tools zu ermöglichen.

  TCP 139, UDP 137 und UDP 138 werden von älteren Protokollen verwendet und sind für aktuelle Anwendungen nicht mehr erforderlich.

  Um den Administrationsserver und die Verteilungspunkte mit den Zielgeräten zu verbinden, müssen in der Firewall dynamische Zugriffsports für ausgehende Daten erlaubt sein.

- Die Sicherheitseinstellungen der Active Directory-Domänenrichtlinie erlauben die Verwendung des NTLM-Protokolls während der Bereitstellung des Administrationsagenten.
- Auf Zielgeräten mit Microsoft Windows XP ist die einfache Dateifreigabe deaktiviert.
- Auf den Zielgeräten ist das Zugriffs- und Sicherheitsmodell auf den Wert *Klassisch – lokale Benutzer authentifizieren sich selbst* eingestellt. Der Wert *Nur Gäste – lokale Benutzer authentifizieren sich als Gast* ist nicht zulässig.
- Die Geräte sind Mitglieder der Domäne oder auf den Geräten wurden bereits einheitliche Benutzerkonten mit Administratorrechten erstellt.

Für die erfolgreiche Bereitstellung des Administrationsagenten oder einer anderen Anwendungen auf einem Gerät, das keiner Active Directory-Domäne von Windows Server 2003 oder höher gehört, müssen Sie die Remote-UAC auf diesem Gerät deaktivieren. Unter anderem aufgrund von Remote-UAC ist es lokalen Administratorkonten nicht möglich, auf die Freigabe "admin$" zuzugreifen. Für die erzwungene Bereitstellung des Administrationsagenten oder anderer Anwendungen ist dieser Zugriff ist jedoch erforderlich. Das Deaktivieren von Remote-UAC hat keine Auswirkungen auf die lokale UAC.

Bei der Installation auf neuen Geräten, die noch nicht in die Administrationsgruppen von Kaspersky Security Center verschoben wurden, kann in den Eigenschaften der Aufgabe zur Remote-Installation die Administrationsgruppe festgelegt werden, in welche die Geräte verschoben werden, nachdem die Installation des Administrationsagenten auf ihnen abgeschlossen wurde.

Beim Erstellen der Gruppenaufgabe muss berücksichtigt werden, dass die Gruppenaufgabe für die Geräte aller angelegten Untergruppen der ausgewählten Gruppe gilt. Deshalb sollten doppelte Installationsaufgaben in den Untergruppen vermieden werden.

Eine vereinfachte Methode zur Erstellung von Aufgaben für eine erzwungene Installation von Anwendungen ist die automatische Installation. Dazu müssen Sie in den Eigenschaften der Administrationsgruppe in der Liste der Installationspakete jene Pakete auswählen, die auf den Geräten dieser Gruppe installiert werden sollen. Daraufhin werden auf allen Geräten dieser Gruppe und ihrer Untergruppen die ausgewählten Installationspakete automatisch installiert. Der Zeitraum, während dem die Pakete installiert werden, hängt von der Netzwerkfähigkeit und der Gesamtmenge der Geräte im Netzwerk ab.

Um die Belastung des Administrationsservers während der Übertragung der Installationspaketen an die Zielgeräte zu reduzieren, können Sie in der Installationsaufgabe die Installationsmethode über Verteilungspunkte auswählen. Beachten Sie dabei, dass diese Installationsmethode eine höhere Belastung für jene Geräte bedeutet, die als Verteilungspunkte agieren. Es wird daher empfohlen, Geräte auszuwählen, die den Voraussetzungen für Verteilungspunkte entsprechen. Sie müssen bei der Verwendung von Verteilungspunkten sicherstellen, dass diese sich in all jenen isolierten Subnetzen befinden, in denen Zielgeräte gehostet werden.

Die Nutzung der Verteilungspunkte als lokale Installationszentren kann auch für die Installation auf Geräten in Subnetzen bequem sein, die mit dem Administrationsserver über einen engen Verbindungskanal verbunden sind, während zwischen den Geräten innerhalb des Subnetzes ein breiter Verbindungskanal verfügbar ist.

Die Größe des freien Speicherplatzes auf der Partition, in der sich der Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit befindet, muss den Gesamtumfang der Programmpakete der zu installierenden Anwendungen um ein Vielfaches übertreffen.

Start der von Kaspersky Security Center gebildeten autonomen Pakete

Die oben beschriebenen Methoden zur erstmaligen Bereitstellung des Administrationsagenten und der Apps können möglicherweise nicht immer durchgeführt werden, da nicht immer alle notwendigen Bedingungen erfüllt werden können. In solchen Fällen kann aus den vom Administrator vorbereiteten Installationspaketen mit den notwendigen Installationseinstellungen mithilfe von Kaspersky Security Center eine einheitliche ausführbare Datei erstellt werden, die als *autonomes Installationspaket* bezeichnet wird. Das autonome Installationspaket kann sowohl auf einem internen Webserver (der Teil von Kaspersky Security Center ist) veröffentlicht werden, wenn dies Sinn macht, wenn also der Zugriff zu diesem Webserver von außen für die Benutzer der Geräte eingerichtet wurde, als auch auf einem speziell bereitgestellten Webserver, der Teil von Kaspersky Security Center Web Console ist. Die autonomen Pakete können auch auf einen anderen Webserver kopiert werden.

Mithilfe von Kaspersky Security Center kann ausgewählten Benutzern per E-Mail ein Link zur Datei des autonomen Pakets auf dem verwendeten Webserver mit der Bitte gesendet werden, die Datei auszuführen (interaktiv oder mit dem Parameter "-s" für die "Silent"-Installation). Das autonome Installationspaket kann für Benutzer von Geräten, die keinen Zugriff auf den Webserver haben, an eine E-Mail-Nachricht angehängt werden. Der Administrator kann außerdem das autonome Paket auf ein externes Gerät kopieren und das Paket zwecks anschließenden Starts an das gewünschte Gerät liefern.

Das autonome Paket kann aus dem Paket des Administrationsagenten, dem Paket anderer Apps (beispielsweise der Sicherheitsanwendung) oder sofort aus beiden Paketen erstellt werden. Wenn das autonome Paket aus dem Administrationsagenten und aus anderen Apps erstellt wurde, beginnt die Installation mit dem Administrationsagenten.

Beim Erstellen des autonomen Paketes mit dem Administrationsagenten kann die Administrationsgruppe angegeben werden, in welche die neuen Geräte (kein Bestandteil der Administrationsgruppen) automatisch nach Abschluss der Installation des Administrationsagenten verschoben werden.

Die autonomen Pakete können interaktiv (standardmäßig), mit Anzeige des Installationsergebnisses der zugehörigen Apps oder im Silent-Modus (beim Start mit dem Parameter "-s") ausgeführt werden. Der Silent-Modus kann für die Installation aus bestimmen Skripts (beispielsweise aus Skripts, die für den Start nach Abschluss der Bereitstellung des Betriebssystem-Images angepasst werden, und ähnliches) verwendet werden. Das Installationsergebnis des Silent-Modus wird durch den Rückgabecode des Prozesses definiert.

Funktion zur manuellen Installation von Apps

Administratoren oder erfahrene Benutzer können die Apps manuell im Interaktivmodus installieren. Dabei können sowohl die originalen Programmpakete als auch die aus ihnen gebildeten Installationspakete verwendet werden, die sich im freigegebenen Ordner Kaspersky Security Center befinden. Die Installer arbeiten standardmäßig im Interaktivmodus und fragen vom Benutzer alle notwendigen Einstellungswerte ab. Beim Start des Prozesses setup.exe aus dem Stamminstallationspaket mit dem Parameter "-s" wird der Installer im Silent-Modus jedoch mit den Einstellungen ausgeführt, die in den Einstellungen des Installationspakets festgelegt wurden.

Beim Start von setup.exe aus dem Stamm des Installationspakets wird das Pakets zuerst in den temporären lokalen Ordner kopiert; anschließend wird der Installer der Anwendung aus der lokalen Hilfe gestartet.

Remote-Installation von Apps auf Geräte mit installiertem Administrationsagenten

Wenn auf dem Gerät ein arbeitsfähiger Administrationsagent installiert ist, der mit dem primären Administrationsserver oder einen seiner sekundären Server verbunden ist, kann auf diesem Gerät die Version des Administrationsagenten aktualisiert werden sowie mithilfe des Administrationsagenten beliebige unterstützte Apps installiert, aktualisiert oder gelöscht werden.

Sie können diese Option aktivieren, indem Sie das Kontrollkästchen **Mithilfe des Administrationsagenten** in den Eigenschaften der Aufgabe zur Remote-Installation aktivieren.

Wenn dieses Kontrollkästchen aktiviert ist, erfolgt die Übertragung der Installationspakete auf die Geräte mit den vom Administrator festgelegten Installationseinstellungen über die Verbindungskanäle zwischen dem Administrationsagenten und dem Administrationsserver.

Zur Optimierung der Belastung auf dem Administrationsserver und zur Verringerung des Datenverkehrs zwischen dem Administrationsserver und den Geräten ist es sinnvoll, in jedem Remote-Netzwerk bzw. in jeder Broadcast-Domäne Verteilungspunkte zu bestimmen (s. Abschnitte Über Verteilungspunkte und Aufbau der Struktur von Administrationsgruppen und Zuweisung von Verteilungspunkten). In diesem Fall erfolgt die Verteilung der Installationspakete und der Einstellungen des Installers vom Administrationsserver auf die Geräte über die Verteilungspunkte.

Unter Verwendung der Verteilungspunkte können auch Broadcast-Domänen (Multicast) den Mailversand der Installationspakete ausführen, wodurch der Netzwerkverkehr während der Bereitstellung der Programme erheblich verringert werden kann.

Bei der Übertragung der Installationspakete auf die Geräte über die Verbindungskanäle zwischen den Administrationsagenten und dem Administrationsserver, werden die zur Sendung vorbereiteten Installationspakete zusätzlich im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer zwischengespeichert. Bei Verwendung einer hohen Anzahl verschiedener Installationspakete mit großem Umfang und bei einer großen Menge von Verteilungspunkten kann die Größe dieses Ordners erheblich zunehmen.

Die Dateien aus dem Ordner FTServer dürfen nicht manuell gelöscht werden. Beim Löschen der Ausgangsinstallationspakete werden die entsprechenden Daten automatisch aus dem Ordner FTServer gelöscht.

Die Daten, die auf der Seite der Verteilungspunkte übernommen werden, werden im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp gespeichert.

Die Dateien aus dem Ordner FTCITmp dürfen nicht manuell gelöscht werden. Je nach Abschluss der Aufgaben, von denen die Daten aus dem Ordner verwendet werden, wird der Inhalt dieses Ordners automatisch gelöscht.

Da die Installationspakete im für das Netzwerk optimalen Format für die Übertragung über die Verbindungskanäle zwischen dem Administrationsserver und den Administrationsagenten aus dem Zwischenspeicher bewegen, dürfen keine Änderungen an den Installationspaketen im ursprünglichen Ordner des Installationspakets vorgenommen werden. Solche Änderungen werden vom Administrationsserver nicht automatisch berücksichtigt. Wenn die Dateien der Installationspakete manuell geändert werden müssen (obwohl das nicht empfohlen wird), müssen unbedingt irgendwelche Einstellungen des Installationspakets in der Verwaltungskonsole geändert werden. Die Änderung der Einstellungen des Installationspakets in der Verwaltungskonsole zwingt den Administrationsserver, das Image des Pakets im Cache zu aktualisieren, das für die Sendung auf die Geräte vorbereitet wurde.

Verwaltung des Neustarts von Geräten in der Aufgabe zur Remote-Installation

Oft wird für den Abschluss der Remote-Installation der App (besonders auf der Plattform Windows) ein Neustart des Geräts gefordert.

Wenn die Aufgabe zur Remote-Installation von Kaspersky Security Center verwendet wird, kann im Assistenten für das Erstellen einer Aufgabe oder im Eigenschaftenfenster der erstellten Aufgabe (Abschnitt **Neustart des Betriebssystems**) die Maßnahme für einen erforderlichen Neustart ausgewählt werden:

- **Gerät nicht neu starten**. In diesem Fall wird kein automatischer Neustart ausgeführt. Für das Abschließen der Installation ist es erforderlich, das Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung der Geräte) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Installationsaufgaben auf Servern und anderen Geräten, für die Störungen während des Arbeitsablaufs kritisch sind.

- **Das Gerät neu starten**. In diesem Fall wird der Neustart immer automatisch ausgeführt, wenn für das Abschließen der Installation ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben zur Installation auf Geräten, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**. In diesem Fall informiert eine Meldung auf dem Client-Gerät den Benutzer darüber, dass das Gerät manuell neu gestartet werden muss. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Die Variante **Benutzer fragen** eignet sich besonders für Workstations, deren Benutzer die Möglichkeit haben sollen, den passendsten Moment für den Neustart auszuwählen.

Zweckdienlichkeit des Datenbanken-Updates im Installationspaket der Antiviren-App

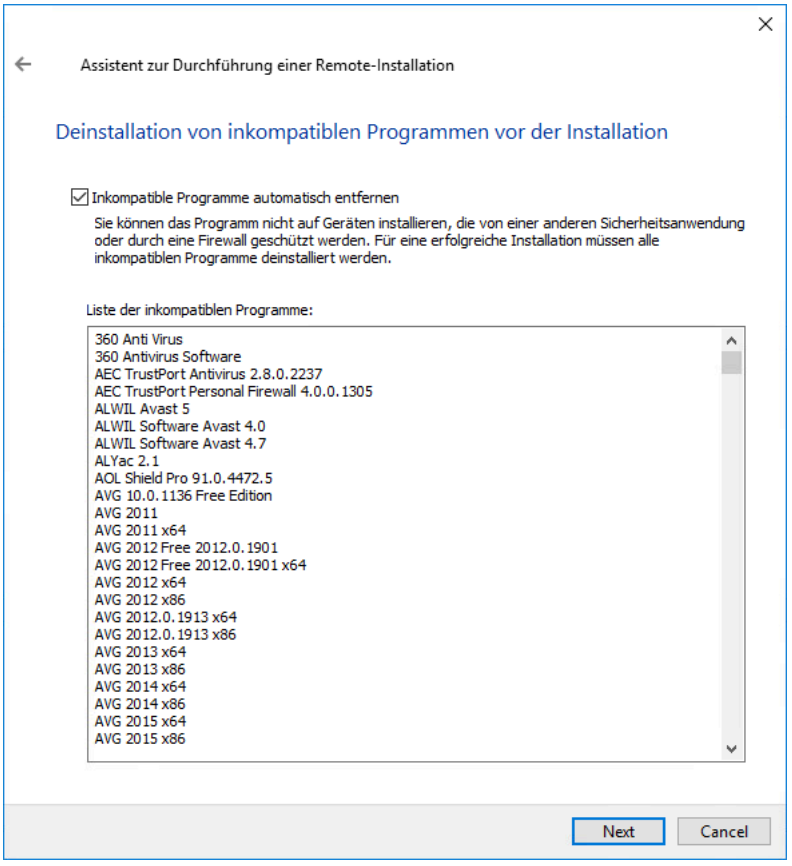
Vor Beginn der Bereitstellung des Schutzes muss die Möglichkeit eines Updates der Antiviren-Datenbanken (einschließlich der Autopatch-Module), die zusammen mit dem Programmpaket der Sicherheitsanwendung bereitgestellt werden, berücksichtigt werden. Es ist zweckmäßig, vor Beginn der Bereitstellung die Datenbanken aus dem Bestand des Installationspakets der App (beispielsweise mithilfe des entsprechenden Befehls im Kontextmenü des ausgewählten Installationspakets) zu aktualisieren. Dadurch wird die Anzahl der Neustarts verringert, die für den Abschluss der Bereitstellung des Schutzes auf den Geräten erforderlich sind. Falls die Installationspakete, die per Relaisübertragung vom primären Administrationsserver an die virtuellen Server weitergeleitet wurden, zur Remote-Installation verwendet werden, müssen die Datenbanken nur im ursprünglichen Paket auf dem primären Administrationsserver aktualisiert werden. Die Datenbanken sollten nicht in den weitergeleiteten Paketen auf den virtuellen Servern aktualisiert werden.

Entfernen der inkompatiblen Sicherheitsanwendungen von Drittanbietern

Zur Installation der Sicherheitsanwendungen von Kaspersky mithilfe von Kaspersky Security Center ist es möglicherweise erforderlich, Drittanbietersoftware zu löschen, die mit dem zu installierenden Programm nicht kompatibel ist. Es existieren zwei Hauptmethoden zur Ausführung dieser Aufgabe.

Automatisches Löschen von inkompatiblen Programmen mithilfe des Installers

Während der Ausführung des Installers bekommen Sie eine Liste mit Programmen angezeigt, die mit einer Kaspersky-Anwendung inkompatibel sind:



Liste mit inkompatiblen Programmen, die im Assistenten für Remote-Installationen angezeigt wird

Kaspersky Security Center spürt inkompatible Programme auf. Infolgedessen können Sie das Kontrollkästchen **Inkompatible Programme automatisch entfernen** aktivieren, um die Installation fortzusetzen. Wenn Sie das Kontrollkästchen nicht aktivieren und die inkompatiblen Programme nicht deinstallieren, wird eine Fehlermeldung angezeigt und die Kaspersky-Anwendung wird nicht installiert.

Das automatische Entfernen inkompatibler Programme wird von verschiedenen Installationsarten unterstützt.

Löschen der inkompatiblen Programme mithilfe einer separaten Aufgabe

Zum Löschen der inkompatiblen Programme wird die Aufgabe *Remote-Deinstallation eines Programms* verwendet. Die Aufgabe muss vor der Aufgabe zur Installation der Sicherheitsanwendung auf den Geräten gestartet werden. Beispielsweise kann in der Installationsaufgabe ein Zeitplan des Typs **Nach Abschluss einer anderen Aufgabe** ausgewählt werden, wobei die andere Aufgabe die Aufgabe *Remote-Deinstallation eines Programms* ist.

Die Verwendung dieser Löschmethode ist zweckmäßig, wenn der Installer der Sicherheitsanwendung eine der inkompatiblen Anwendungen nicht erfolgreich löschen kann.

Einen kennwortgeschützten Administrationsagenten über die Eingabeaufforderung entfernen

Um einen Administrationsagenten, für den Sie ein Deinstallationskennwort festgelegt haben, remote zu deinstallieren, können Sie die Eingabeaufforderung verwenden.

> Wenn Sie für einen kennwortgeschützten Administrationsagenten auf einem Gerät, das nicht mehr von Kaspersky Security Center verwaltet wird, das Kennwort verlieren oder vergessen, können Sie diesen Administrationsagenten weder mit den Tools "klmover" und "Cleaner" (cleaner.exe) noch über die Eingabeaufforderung entfernen. In diesem Fall müssen Sie auf dem Gerät mit installiertem kennwortgeschützten Administrationsagenten das Betriebssystem neu installieren.

So entfernen Sie den Administrationsagenten über die Eingabeaufforderung:

1. Wandeln Sie Ihr Deinstallationskennwort in einen Hex-Code um.

   Verwenden Sie eine Internetressource, eine Programmierumgebung, einen Texteditor oder ein anderes geeignetes Tool, um Ihr Kennwort in Hex-Code umzuwandeln.

   > Stellen Sie sicher, dass das zum Separieren des generierten Hex-Codes die verwendete Ausgabetrennzeichen auf `00` gesetzt ist. Beispiel: Der Hex-Code `51 77 65 72 74 79` nicht korrekt und der Hex-Code `510077006500720074007900` korrekt.

2. Geben Sie den folgenden Befehl in der Eingabeaufforderung ein und drücken Sie anschließend die **`EINGABETASTE`**:

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   Sie können den Produktcode Ihres Administrationsagenten der folgenden Tabelle entnehmen:

   Produktcodes der Administrationsagenten

Sprachversion	Produktcode
Arabisch	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}

Bulgarisch	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
Tschechisch	{478A6A0B-D177-4402-B703-808C05C56B13}
Englisch	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
Französisch	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
Deutsch	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
Ungarisch	{8899A4D4-D678-49F8-AD96-0B784F58D355}
Italienisch	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
Japanisch	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
Koreanisch	{70812A40-973B-4DA1-96B9-C2011280CD99}
Polnisch	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
Portugiesisch	{0F05E4E5-5A89-482C-9A62-47CC58643788}
Rumänisch	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
Russisch	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
Vereinfachtes Chinesisch	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
Spanisch	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
Spanisch-mx	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
Traditionelles Chinesisch	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
Türkisch	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Verwendung von Tools zur Remote-Installation der Apps von Kaspersky Security Center für den Start von beliebigen ausführbaren Dateien auf den verwalteten Geräten

Mithilfe des Assistenten für das Erstellen eines Installationspakets kann eine beliebige ausführbare Datei ausgewählt und dafür die Befehlszeilenparameter festlegt werden. Dabei können im Installationspaket sowohl die ausgewählte Datei als auch der gesamte Ordner, in dem diese Datei enthalten ist, untergebracht werden. Anschließend muss die Aufgabe zur Remote-Installation erstellt und das erstellte Installationspaket ausgewählt werden.

Während der Ausführung der Aufgabe auf den Geräten wird die beim Erstellen angegebene ausführbare Datei mit den aufgegebenen Befehlszeilenparametern ausgeführt.

Wenn Installer im Format Microsoft Windows Installer (MSI) verwendet werden, verwendet Kaspersky Security Center die Standardmöglichkeiten gemäß der Analyse des Installationsergebnisses.

Wenn eine Lizenz für Schwachstellen- und Patch-Management vorhanden ist, verwendet Kaspersky Security Center beim Erstellen des Installationspakets für eine der unterstützten Apps, die in der Unternehmensumgebung verteilt sind, auch die Regeln zur Installation und Analyse der Installationsergebnisse, die in der aktualisierten Datenbank vorhanden sind.

In allen anderen Fälle wartet die Aufgabe bei ausführbaren Dateien standardmäßig auf den Abschluss des ausgeführten Prozesses und aller dadurch generierten untergeordneten Prozesse. Nach dem Abschluss der ausgeführten Prozesse wird die Aufgabe unabhängig vom Rückgabecode des Ausgangsprozesses erfolgreich beendet. Um ein solches Verhalten der Aufgabe zu ändern, müssen vor dem Erstellen der Aufgabe die kpd-Dateien, die von Kaspersky Security Center im Ordner des neu erstellten Installationspakets, sowie dessen Unterordnern, erzeugt wurden, manuell geändert werden.

Für .kpd-Dateien wird die ASCII-Kodierung verwendet, während für .kud-Dateien die Unicode-Kodierung verwendet wird.

Damit die Aufgabe den Abschluss des ausgeführten Prozesses nicht abwartet, muss im Abschnitt [SetupProcessResult] für die Einstellung Wait der Wert 0 festgelegt werden:

```
[SetupProcessResult]
Wait=0
```

Damit die Aufgabe auf der Windows-Plattform nur den Abschluss des Ausgangsprozesses, aber nicht der von ihm erzeugten untergeordneten Prozesse abwartet, muss in Abschnitt [SetupProcessResult] für die Einstellung WaitJob der Wert 0 festgelegt werden, zum Beispiel:

```
[SetupProcessResult]
WaitJob=0
```

Damit die Aufgabe erfolgreich abgeschlossen wird oder je nach Rückgabecode des laufenden Prozesses einen Fehler ausgibt, erstellen Sie eine ausführbare .bat-Datei, die den Fehlercode in einer Datei speichert, zum Beispiel:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Ändern Sie anschließend außerdem die .kud-Dateien, die von Kaspersky Security Center im Ordner des neu erstellten Installationspakets generiert wurden:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

In diesem Fall wird ein beliebiger, sich von den aufgezählten unterscheidender, Code auf einen Fehler hindeuten.

Damit in den Ergebnissen der Aufgabe eine Zeile mit einem Kommentar über den erfolgreichen Abschluss der Aufgabe bzw. der Fehlerdiagnose angezeigt wird, müssen in den Abschnitten [SetupProcessResult_SuccessCodes] und [SetupProcessResult_ErrorCodes] kurze Fehlerbeschreibungen, die den Rückgabecodes des Prozesses entsprechen, festgelegt werden, zum Beispiel:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
```

```
1602=Installation canceled by the user
1603=Fatal error during installation
```

Damit die Tools von Kaspersky Security Center zur Verwaltung des Neustarts des Geräts eingesetzt werden können (wenn ein Neustart für den Abschluss der Operation erforderlich ist), müssen im Abschnitt [SetupProcessResult_NeedReboot] zusätzlich die Rückgabecodes des Prozesses, die einen erforderlichen Neustart bedeuten, aufgezählt werden:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitoring der Bereitstellung

Zur Kontrolle der Bereitstellung von Kaspersky Security Center sowie zur Überprüfung auf eine vorhandene Sicherheitsanwendung auf den verwalteten Geräten und des Administrationsagenten, müssen die farblichen Kennzeichnungen im Block **Bereitstellung** beachtet werden. Die Kennzeichnung befindet sich im Arbeitsbereich des Administrationsserver-Knotens im Hauptfenster der Verwaltungskonsole. Die Kennzeichnung zeigt aktuellen Status der Bereitstellung an. Neben der Kennzeichnung wird die Anzahl der Geräte mit installiertem Administrationsagenten und Sicherheitsanwendungen angezeigt. Bei vorhandenen aktiven Installationsaufgaben wird der Ausführungsfortschritt der Aufgaben angezeigt. Bei etwaigen Installationsfehlern wird die Anzahl der Fehler angezeigt und über einen Link besteht die Möglichkeit zur Anzeige ausführlichen Informationen über den Fehler. Farbliche Kennzeichnungen in der Verwaltungskonsole.

Es gibt ferner die Möglichkeit, im Arbeitsbereich des Ordners **Verwaltete Geräte** auf der Registerkarte **Gruppen** ein Diagramm der Bereitstellung anzuzeigen. Das Diagramm gibt den Verteilungsprozess wieder, indem es die Anzahl der Geräte ohne Administrationsagent, mit Administrationsagent, und mit Administrationsagenten und Sicherheitsanwendung anzeigt.

Eine ausführlichere Beschreibung des Verlaufs der Bereitstellung (bzw. der Ausführung einer konkreten Installationsaufgabe) wird im Ergebnisfenster für die Ausführung der entsprechenden Aufgabe der Remote-Installation angezeigt. Das Ergebnisfenster ist über das Kontextmenü der Aufgabe (Punkt **Ergebnisse**) verfügbar. Im Fenster werden zwei Listen angezeigt: die obere Liste enthält eine Auflistung der Status der Aufgabe auf den Geräten, und in der unteren wird die Ereignisliste für die Aufgabe auf dem Gerät angezeigt, das in der oberen Liste derzeit ausgewählt ist.

Die Informationen über Fehler bei der Bereitstellung werden im Kaspersky-Ereignisprotokoll des Administrationsservers gespeichert. Die Informationen über Fehler sind auch in der entsprechenden Ereignisauswahl im Ordner **Berichte und Benachrichtigungen** im Unterordner **Ereignisse** verfügbar.

Anpassen der Einstellungen der Installer

Dieser Abschnitt enthält Informationen über die Dateien der Installer von Kaspersky Security Center und die Installationseinstellungen sowie Empfehlung zur Installation des Administrationsservers und des Administrationsagenten im Silent-Modus.

Allgemeine Informationen

Die Installer von Kaspersky Security Center 15.1 (Administrationsserver, Administrationsagent, Verwaltungskonsole) sind auf der Technologie des Windows Installers aufgebaut. Der Kern des Installers ist das MSI-Paket. Dieses Verpackungsformat der Distribution erlaubt, alle Vorteile der Windows Installer-Technologie zu verwenden: die Skalierbarkeit, die Möglichkeit von System-Patches, das System der Transformation, die Möglichkeit einer zentralisierten Installation von Drittanbieter-Lösungen, die Transparenz der Anmeldung im Betriebssystem.

Installation im Silent-Modus (mit Antwortdatei)

In den Installern des Administrationsservers und des Administrationsagenten gibt es die Möglichkeit zur Verwendung der Antwortdatei (ss_install.xml), in der die Parameter für die Installation im Silent-Modus ohne Benutzerinteraktion gespeichert sind. Die Datei ss_install.xml befindet sich im selben Ordner wie das msi-Paket und wird automatisch bei der Installation im Silent-Modus verwendet. Sie können die Installation im Silent-Modus mit dem Befehlszeilenparameter "/ s" aktivieren.

Beispiel für den Start:

```
setup.exe /s
```

Lesen Sie den Endbenutzer-Lizenzvertrag (EULA), bevor Sie das Installationsprogramm im Silent-Modus starten. Wenn das Programmpaket von Kaspersky Security Center keine txt-Datei mit dem Text der EULA enthält, können Sie die Datei auf der Website von Kaspersky herunterladen.

Die Datei ss_install.xml stellt eine Instanz des internen Formats für die Parameter des Installers für Kaspersky Security Center dar. Im Lieferumfang der Programmpakete wird die Datei ss_install.xml mit den Standardparametern geliefert.

Die Datei ss_install.xml darf nicht manuell geändert werden. Diese Datei wird mithilfe von Kaspersky Security Center bei der Änderung der Parameter der Installationspakete in der Verwaltungskonsole geändert.

So ändern Sie die Antwortdatei für die Installation des Administrationsservers:

1. Öffnen Sie das Programmpaket von Kaspersky Security Center. Wenn Sie eine exe-Datei für das Komplettpaket verwenden, entpacken Sie diese.
2. Öffnen Sie ausgehend vom Server-Ordner die Befehlszeile und führen Sie anschließend den folgenden Befehl aus:
   ```
   setup.exe /r ss_install.xml
   ```
   Das Installationsprogramm von Kaspersky Security Center wird gestartet.
3. Folgen Sie den Schritten des Assistenten, um die Installation von Kaspersky Security Center zu konfigurieren.

   Wenn Sie den Assistenten abschließen, wird die Antwortdatei automatisch gemäß den neuen Einstellungen geändert, die Sie angegeben haben.

Installation des Administrationsagenten im Silent-Modus (ohne Antwortdatei)

Der Administrationsagent kann nur mithilfe eines msi-Pakets installiert werden, dabei werden die Werte der MSI-Eigenschaften MSI standardmäßig festgelegt. Ein solches Szenario erlaubt, den Administrationsagenten unter Verwendung von Gruppenrichtlinien zu installieren.

Benennen Sie das Installationspaket "Kaspersky Network Agent.msi" nicht um. Ein Umbenennen dieses Pakets kann bei zukünftigen Updates des Administrationsagenten zu Installationsfehlern führen.

Damit kein Konflikt zwischen den Parametern, die mithilfe der MSI-Eigenschaften festgelegt wurden, und den Parametern, die in der Antwortdatei festgelegt sind, entsteht, kann die Antwortdatei mittels Angabe der Eigenschaft `DONT_USE_ANSWER_FILE=1` deaktiviert werden. Die msi-Datei befindet sich im Programmpaket für Kaspersky Security Center im Ordner Packages\NetAgent\exec. Nachfolgend ist ein Beispiel für den Start des Installers des Administrationsagenten mithilfe des msi-Paketes angeführt.

Für die Installation des Administrationsagenten im Silent-Modus müssen die Bedingungen des Endbenutzer-Lizenzvertrags akzeptiert werden. Verwenden Sie den Parameter `EULA=1` nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen haben, und sie verstehen und akzeptieren.

Beispiel:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Sie können die Parameter zur Installation des msi-Paketes auch festlegen, indem Sie eine temporäre Transformationsdatei vorbereiten (Datei mit der Erweiterung mst). Der Befehl sieht folgendermaßen aus:

Beispiel:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

In einem Befehl können mehrere Transformationsdateien angegeben werden.

Wenn Sie den Administrationsagenten mithilfe von Windows Installer aktualisieren möchten, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Teilweises Anpassen der Installationseinstellungen durch setup.exe

Beim Start der Programminstallation mittels setup.exe können die Werte beliebiger MSI-Eigenschaften ins msi-Paket übergeben werden.

Der Befehl sieht folgendermaßen aus:

Beispiel:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Installationseinstellungen für den Administrationsserver

In der nachfolgenden Tabelle werden die MSI-Eigenschaften beschrieben, die bei der Installation des Administrationsservers angepasst werden können. Alle Parameter mit Ausnahme von EULA und PRIVACYPOLICY sind optional.

MSI-Eigenschaft	Beschreibung	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Lizenzvertrags (obligatorische Einstellung)	• 1 – Ich habe die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen, und verstehe und akzeptiere sie. • Anderer Wert oder keine Angabe – die Bedingungen des Endbenutzer-Lizenzvertrags werden abgelehnt (die Installation wird nicht ausgeführt).
PRIVACYPOLICY	Einverständnis mit den Bedingungen der Datenschutzrichtlinie (obligatorische Einstellung)	• 1 – Mir ist bewusst und ich bin damit einverstanden, dass meine Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Ich bestätige, dass ich die Datenschutzrichtlinie vollständig gelesen habe und sie verstehe. • Anderer Wert oder keine Angabe – die Bedingungen der Datenschutzrichtlinie werden abgelehnt (die Installation wird nicht ausgeführt).
INSTALLATIONMODETYPE	Installationstyp für den Administrationsserver	• Standard. • Benutzerdefiniert.
INSTALLDIR	Ordner der Programminstallation	Zeichenfolgenwert.
ADDLOCAL	Liste der Installationskomponenten (kommagetrennt)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Liste der Komponenten, die als Mindestvoraussetzungen für eine korrekte Installation des Administrationsservers gelten: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Netzwerkgröße	• NRT_1_100 – von 1 bis 100 Geräte • NRT_100_1000 – von 101 bis 1.000 Geräte • NRT_GREATER_1000 – mehr als 1.000 Geräte
SRV_ACCOUNT_TYPE	Art der Angabe des Benutzers für die Ausführung des Dienstes des Administrationsservers	• SrvAccountDefault – das Benutzerkonto wird automatisch erstellt. • SrvAccountUser – das Benutzerkonto wird manuell festgelegt.
SERVERACCOUNTNAME	Benutzername für den Dienst	Zeichenfolgenwert.
SERVERACCOUNTPWD	Benutzerkennwort für den Dienst	Zeichenfolgenwert.
DBTYPE	Typ der Datenbank	• MySQL – Eine MySQL- oder MariaDB-Datenbank wird verwendet. • MSSQL – Eine Datenbank des Typs Microsoft SQL Server (SQL Express) wird verwendet.
MYSQLSERVERNAME	Vollständiger Name des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MYSQLSERVERPORT	Portnummer für die Verbindung mit dem MySQL- oder MariaDB-Server	Zahlenwert.
MYSQLDBNAME	Name der Datenbank des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MYSQLACCOUNTNAME	Benutzername für die Verbindung mit der Datenbank des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MYSQLACCOUNTPWD	Benutzerkennwort für die Verbindung mit der Datenbank des MySQL- oder MariaDB-Servers	Zeichenfolgenwert.
MSSQLCONNECTIONTYPE	Verwendungstyp der MSSQL-Datenbank	• InstallMSSEE – aus einem Paket installieren. • ChooseExisting – installierten Server verwenden.
MSSQLSERVERNAME	Vollständiger Name der SQL Server-Instanz	Zeichenfolgenwert.
MSSQLDBNAME	Name der Datenbank von SQL Server	Zeichenfolgenwert.
MSSQLAUTHTYPE	Authentifizierungsmethode bei der Verbindung mit SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Benutzername für die Verbindung zu SQL Server im Modus SQLServer	Zeichenfolgenwert.

MSI-Eigenschaft	Beschreibung	Mögliche Werte
MSSQLACCOUNTPWD	Benutzerkennwort für die Verbindung zu SQL Server im Modus SQLServer	Zeichenfolgenwert.
CREATE_SHARE_TYPE	Methode zum Erstellen eines gemeinsamen Ordners	• Create – neuen freigegebenen Ordner erstellen. In diesem Fall müssen folgende Eigenschaften festgelegt werden: • SHARELOCALPATH – Pfad zu einem lokalen Ordner. • SHAREFOLDERNAME – Netzwerkname eines Ordners. • Null – die Eigenschaft EXISTSHAREFOLDERNAME muss festgelegt werden.
EXISTSHAREFOLDERNAME	Vollständiger Name eines vorhandenen gemeinsamen Ordners	Zeichenfolgenwert.
SERVERPORT	Portnummer für das Herstellen einer Verbindung mit dem Administrationsserver	Zahlenwert.
SERVERSSLPORT	Port für die Installation der SSL-Verbindung mit dem Administrationsserver	Zahlenwert.
SERVERADDRESS	Adresse des Administrationsservers	Zeichenfolgenwert.
SERVERCERT2048BITS	Die Lange des Schlüssels für das Zertifikat des Administrationsservers (in Bits)	• 1 – die Länge des Schlüssels für das Zertifikat des Administrationsservers beträgt 2048 Bit. • 0 – die Länge des Schlüssels für das Zertifikat des Administrationsservers beträgt 1024 Bit. • Wenn kein Wert angegeben ist, beträgt die Länge des Schlüssels für das Zertifikat des Administrationsservers 2.024 Bit.
MOBILESERVERADDRESS	Adresse des Administrationsservers zum Verbinden mit mobilen Geräten; wird ignoriert, wenn die Komponente "MobileSupport" nicht ausgewählt ist	Zeichenfolgenwert.

Installationseinstellungen des Administrationsagenten

In der nachfolgenden Tabelle werden die MSI-Eigenschaften beschrieben, die bei der Installation des Administrationsagenten angepasst werden können. Alle Parameter mit Ausnahme SERVERADDRESS sind optional.

MSI-Eigenschaften

MSI-Eigenschaft	Beschreibung	Mögliche Werte
DONT_USE_ANSWER_FILE	Installationsparameter aus der Antwortdatei lesen	• 1 • Leer
INSTALLDIR	Installationsordner	
SERVERADDRESS	Adresse des Administrationsservers (obligatorische Einstellung)	
SERVERPORT	Port zum Herstellen einer Verbindung mit dem Administrationsserver	
SERVERSSLPORT	Portnummer der SSL-Verbindung	
USESSL	Soll eine SSL-Verbindung verwendet werden?	• 1 • Leer
OPENUDPPORT	Soll ein UDP-Port geöffnet werden?	• 1 • Leer
UDPPORT	UDP-Port	
USEPROXY	Soll ein Proxyserver verwendet werden?	• 1 • Leer
PROXYADDRESS	Proxy-Adresse	
PROXYPORT	Portnummer der Verbindung zum Administrationsserver	

MSI-Eigenschaft	Beschreibung	Mögliche Werte
PROXYLOGIN	Benutzerkonto zur Verbindung mit dem Proxyserver.	
PROXYPASSWORD	Kennwort des Benutzerkontos zur Verbindung mit dem Proxyserver. Geben Sie in den Einstellungen der Installationspakete keine Daten von privilegierten Benutzerkonten an.	
GATEWAYMODE	Modus für die Nutzung eines Verbindungs-Gateways	• 0 – Kein Verbindungs-Gateway verwenden • 1 – Diesen Administrationsagenten als Verbindungs-Gateway verwenden • 2 – Verbindung zum Administrationsserver mittels Verbindungs-Gateway herstellen
GATEWAYADDRESS	Verbindungs-Gateway-Adresse	
CERTSELECTION	Methode zum Anfordern eines Zertifikats	• GetOnFirstConnection – Zertifikat vom Administrationsserver anfordern • GetExistent – Bestehendes Zertifikat auswählen. Wenn diese Option ausgewählt ist, muss die Eigenschaft CERTFILE definiert werden.
CERTFILE	Pfad der Zertifikatsdatei	
VMVDI	Dynamischen Modus für VDI aktivieren	• 1 • Leer
LAUNCHPROGRAM	Legt fest, ob der Dienst des Administrationsagenten nach der Installation gestartet werden soll	• 1 • Leer

Virtuelle Infrastruktur

Kaspersky Security Center unterstützt die Arbeit mit virtuellen Maschinen. Sie können den Administrationsagenten und die Sicherheitsanwendungen auf jeder virtuellen Maschine installieren und virtuelle Maschinen auf Hypervisor-Ebene schützten. Im ersten Fall kann sowohl die Standard-Sicherheitsanwendung als auch Kaspersky Security for Virtualization Light Agent für den Schutz der virtuellen Maschinen verwendet werden. Im zweiten Fall kann Kaspersky Security for Virtualization Agentless verwendet werden.

Kaspersky Security Center unterstützt das Rollback von virtuellen Maschinen auf ihren vorherigen Zustand.

Empfehlungen zur Senkung der Belastung auf den virtuellen Maschinen

Wenn der Administrationsagent auf einer virtuellen Maschine installiert wird, muss eine Möglichkeit zum Deaktivieren jenes Teils der Funktionalität von Kaspersky Security Center vorgesehen werden, der für die virtuellen Maschinen von geringem Wert ist.

Bei der Installation des Administrationsagenten auf einer virtuellen Maschine oder einer Vorlage, aus der virtuelle Maschinen erstellt werden sollen, ist es empfehlenswert, wie folgt vorzugehen:

- Wenn eine Remote-Installation ausgeführt wird, wählen Sie im Eigenschaftenfenster für das Installationspaket des Administrationsagenten im Abschnitt **Erweitert** die Option **Einstellungen für VDI optimieren** aus.
- Wenn mithilfe des Assistenten eine interaktive Installation ausgeführt wird, wählen Sie im Fenster des Assistenten die Option **Einstellungen des Administrationsagenten für die virtuelle Infrastruktur optimieren** aus.

Durch Auswählen der Optionen werden die Einstellungen des Administrationsagenten so geändert, dass standardmäßig die folgenden Funktionen deaktiviert werden (bevor eine Richtlinie angewendet wird):

- Informationen über die installierte Software empfangen
- Informationen über die Hardware empfangen
- Informationen über vorhandene Schwachstellen empfangen
- Informationen über erforderliche Updates empfangen

Üblicherweise müssen die aufgezählten Funktionen auf den virtuellen Maschinen nicht aktiviert sein, damit die Software und die virtuelle Hardware darauf einheitlich sind.

Das Deaktivieren der Funktionen kann rückgängig gemacht werden. Wenn eine der deaktivierten Funktionen doch erforderlich ist, kann sie mithilfe der Richtlinie des Administrationsagenten oder in den lokalen Einstellungen des Administrationsagenten aktiviert werden. Die lokalen Einstellungen des Administrationsagenten sind über das Kontextmenü des entsprechenden Geräts in der Verwaltungskonsole verfügbar.

Unterstützung von dynamischen virtuellen Maschinen

Kaspersky Security Center unterstützt dynamische virtuelle Maschinen. Wenn im Netzwerk des Unternehmens eine virtuelle Infrastruktur implementiert ist, können in einigen Fällen dynamische (temporärer) virtuellen Maschinen verwendet werden. Solche Maschinen werden mit eindeutigen Namen aus einer vom Administrator im Voraus vorbereiteten Vorlage erstellt. Der Benutzer arbeitet eine gewisse Zeit auf einer VM und nach dem Deaktivieren wird die virtuelle Maschinen aus der virtuellen Infrastruktur entfernt. Wenn im Netzwerk des Unternehmens Kaspersky Security Center implementiert ist, wird die virtuelle Maschine mit darauf installiertem Administrationsagenten zur Administrationsserver-Datenbank hinzugefügt. Nach dem Deaktivieren der virtuellen Maschine muss der sie betreffende Eintrag auch aus der Datenbank des Administrationsservers gelöscht werden.

Damit die Funktionalität des automatischen Löschens der Einträge über virtuelle Maschinen bei der Installation des Administrationsagenten auf der Vorlage, aus der die dynamischen virtuellen Maschinen erstellt werden, funktioniert, muss die Option **Dynamischen Modus für VDI aktivieren** aktiviert werden:

- Im Falle einer Remote-Installation im Eigenschaftenfenster des Installationspakets des Administrationsagenten (Abschnitt **Erweitert**)
- Für die interaktive Installation – im Installationsassistenten des Administrationsagenten

> Die Option **Dynamischen Modus für VDI aktivieren** muss bei der Installation des Administrationsagenten auf realen Geräten nicht aktiviert werden.

Wenn es erforderlich ist, dass Ereignisse auf dynamischen virtuellen Maschinen eine bestimmte Zeit nach dem Löschen der Maschinen auf dem Administrationsserver gespeichert werden, muss im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignis-Datenverwaltung** die Option **Ereignisse von gelöschten Geräten weiterhin speichern** aktiviert und die maximale Speicherdauer der Ereignisse in Tagen angegeben werden.

> Es wird davon abgeraten, die Verschlüsselung von Laufwerken auf dynamischen virtuellen Maschinen zu aktivieren.

Unterstützung des Kopierens von virtuellen Maschinen

Das Kopieren von virtuellen Maschine mit darauf installiertem Administrationsagenten oder deren Erstellung aus einer Vorlage mit installiertem Administrationsagenten entspricht der Bereitstellung der Administrationsagenten durch Aufzeichnen und Kopieren eines Festplatten-Image. Deshalb muss man im Allgemeinen beim Kopieren von virtuellen Maschinen dieselbe Aktion ausführen wie bei der Bereitstellung des Administrationsagenten durch Kopieren eines Images der Festplatte.

In den nachstehend beschriebenen beiden Fällen erkennt der Administrationsagent die Tatsache des Kopierens allerdings automatisch. Deshalb ist die Ausführung der komplizierten Aktionen, die in im Abschnitt "die Bereitstellung durch Aufzeichnen und Kopieren der Festplatte des Geräts" nicht obligatorisch:

- Bei der Installation des Administrationsagenten war die Option **Dynamischen Modus für VDI aktivieren** aktiviert: nach jedem Neustart des Betriebssystems wird eine solche virtuelle Maschine unabhängig von der Tatsache, dass sie kopiert wurde, als neues Gerät betrachtet.

- Es wird einer der folgenden Hypervisoren verwendet: VMware™, HyperV oder Xen: der Administrationsagent erkennt die Tatsache des Kopierens der virtuellen Maschine anhand der geänderten ID der virtuellen Hardware.

Die Analyse der Änderungen der virtuellen Hardware ist nicht absolut sicher. Bevor die vorliegende Methode umfassend verwendet wird, muss zuvor ihre Funktionsfähigkeit für die im Unternehmen verwendete Version des Hypervisors auf einer kleinen Anzahl virtueller Maschinen geprüft werden.

Unterstützung des Rollbacks des Dateisystems für Geräte mit Administrationsagent

Kaspersky Security Center ist ein verteiltes Programm. Ein Rollback des Dateisystems auf den vorhergehenden Zustand auf einem der Geräte mit installiertem Administrationsagenten führt zu einer Desynchronisierung der Daten und zur fehlerhaften Ausführung von Kaspersky Security Center.

Ein Rollback des Dateisystems (oder eines Teils davon) auf den vorhergehenden Zustand kann in folgenden Fälle durchgeführt werden:

- Beim Kopieren eines Festplatten-Image.

- Bei der Wiederherstellung des Status der virtuellen Maschine mithilfe der virtuellen Infrastruktur.

- Beim Wiederherstellen der Daten aus der Backup-Kopie oder einem Wiederherstellungspunkt.

Szenarios, in denen Drittanbieter-Programme auf Geräten mit installiertem Administrationsagenten den Ordner "%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\" betreffen, stellen nur für Kaspersky Security Center kritische Szenarios dar. Deshalb ist es erforderlich, diesen Ordner, wenn möglich immer aus der Wiederherstellungsprozedur auszuschließen.

Da in einer Reihe von Unternehmen die Dienstordnung das Ausführen eines Rollbacks des Zustandes des Dateisystems der Geräte voraussetzt, wurde in Kaspersky Security Center ab Version 10 Maintenance Release 1 (Administrationsserver und die Administrationsagenten müssen Versionen 10 Maintenance Release 1 oder höher sein) die Unterstützung der Erkennung eines Rollbacks des Dateisystems auf den Geräten mit installiertem Administrationsagenten hinzugefügt. Im Fall des Erkennens werden solche Geräte automatisch mit einem Administrationsserver mit vollständiger Bereinigung und vollständiger Synchronisierung der Daten verbunden.

In Kaspersky Security Center 15.1 ist die Unterstützung des Erkennens eines Rollbacks des Dateisystems standardmäßig aktiviert.

Falls irgendwie möglich, muss ein Rollback des Ordners %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ auf den Geräten mit installiertem Administrationsagenten vermieden werden, da eine nochmalige vollständige Synchronisierung der Daten einen großen Teil der Ressourcen fordert.

Für das Gerät mit installiertem Administrationsserver ist ein Rollback des Systemzustands unzulässig. Ebenfalls unzulässig ist ein Rollback auf den vorhergehenden Zustand der Datenbank, die vom Administrationsserver verwendet wird.

Der Zustand des Administrationsservers kann nur mithilfe des Standardtools klbackup aus der Backup-Kopie wiederhergestellt werden.

Über Verbindungsprofile für mobile Benutzer

Bei der Arbeit der mobilen Benutzer, die Laptops (im Weiteren auch "Geräte") verwenden, kann es erforderlich sein, die Verbindungsmethode mit dem Administrationsserver zu ändern oder abhängig von aktuellen Standort des Geräts im Netzwerk zwischen Administrationsservern umzuschalten.

Verbindungsprofile werden nur für Geräte mir Windows oder macOS unterstützt.

Nutzung verschiedener Adressen ein- und desselben Administrationsservers

Die Geräte mit installiertem Administrationsagenten können in unterschiedlichen Zeiträumen sowohl aus dem internen Netzwerk des Unternehmens als auch aus dem Internet mit dem Administrationsserver verbunden werden. In dieser Situation kann es erforderlich sein, dass der Administrationsagent verschiedene Adressen für die Verbindung mit dem Administrationsserver verwendet: die externe Adresse des Servers bei der Verbindung aus dem Internet und die interne Adresse des Servers bei der Verbindung aus dem internen Netzwerk.

Dazu müssen Sie ein Profil (zur Verbindung mit dem Administrationsserver aus dem Internet) zur Richtlinie des Administrationsagenten hinzufügen. Fügen Sie das Profil in den Richtlinieneigenschaften (Abschnitt **Konnektivität**, Unterabschnitt **Verbindungsprofile**) hinzu. Deaktivieren Sie im Fenster für die Profilerstellung die Option **Nur für Update-Download verwenden** und aktivieren Sie die Option **Verbindungseinstellungen mit den Einstellungen für den Administrationsserver synchronisieren, die in diesem Profil angegeben sind**. Wenn für den Zugriff auf den Administrationsserver ein Verbindungs-Gateway verwendet wird (beispielsweise in einer Konfiguration von Kaspersky Security Center vom Typ Zugriff aus dem Internet: Administrationsagent als Verbindungs-Gateway in der demilitarisierten Zone), muss im Verbindungsprofil die Adresse des Verbindungs-Gateways im entsprechenden Feld angegeben werden.

Umschaltung zwischen Administrationsservern in Abhängigkeit vom aktuellen Netzwerk

Wenn es im Unternehmen mehrere Büros mit verschiedenen Administrationsservern gibt und zwischen ihnen ein Teil der Geräte mit installiertem Administrationsagenten verschoben wird, ist es erforderlich, dass der Administrationsagent mit dem Administrationsserver des lokalen Netzwerkes jenes Büros verbunden wird, in dem sich das Gerät befindet.

In diesem Fall ist es erforderlich, in den Eigenschaften der Richtlinie des Administrationsagenten das Profil für Verbindung mit Administrationsserver für jedes der Büros mit Ausnahme des Büros zu erstellen, in dem sich der Home-Administrationsserver befindet. In den Verbindungsprofilen müssen die Adressen der entsprechenden Administrationsserver angegeben werden und die Option **Nur für Update-Download verwenden** entweder aktiviert oder deaktiviert werden:

- Aktivieren Sie die Option, wenn es erforderlich ist, dass sich der Administrationsagent mit dem Home-Administrationsserver synchronisiert und der lokale Server nur für den Update-Download verwendet wird.
- Deaktivieren Sie diese Option, wenn erforderlich ist, dass der Administrationsagent den lokalen Administrationsserver vollständig verwaltet.

Des Weiteren müssen die Bedingungen für die Umschaltung auf die erstellten Profile angepasst werden: mindestens eine Bedingung für jedes Büro, mit Ausnahme des "Home-Office". Der Sinn jeder solchen Bedingung besteht in der Sichtbarkeit der büroeigenen Details in der Netzwerkumgebung. Wenn eine Bedingung erfüllt wird, erfolgt die Aktivierung des entsprechenden Profils. Trifft keine der Bedingungen zu, wird der Administrationsagent auf den Home-Administrationsserver umgeschaltet.

Bereitstellung der Funktionalität "Verwaltung mobiler Geräte"

Dieser Abschnitt enthält Informationen über die erstmalige Bereitstellung der Funktion "Verwaltung mobiler Geräte".

Verbindung von KES-Geräten mit dem Administrationsserver

Abhängig von der Verbindungsmethode der Geräte mit dem Administrationsserver existieren zwei Bereitstellungsschemas von Kaspersky Device Management für iOS für KES-Geräte:

- Bereitstellungsschema unter Verwendung einer direkten Verbindung der Geräte mit dem Administrationsserver
- Schema für die Bereitstellung mit einem Reverse-Proxy, der die eingeschränkte Delegierung von Kerberos unterstützt

Direkte Verbindung der Geräte mit dem Administrationsserver

KES-Geräte können direkt mit dem Port 13292 des Administrationsservers verbunden werden.

Abhängig von der Art der Authentifizierung existieren zwei Varianten zur Verbindung von KES-Geräten mit dem Administrationsserver:

- Verbindung der Geräte unter Verwendung eines Benutzerzertifikats
- Verbindung der Geräte ohne Benutzerzertifikat

Verbindung eines Geräts unter Verbindung eines Benutzerzertifikats

Bei der Verbindung eines Geräts unter Verwendung eines Benutzerzertifikats erfolgt ein Anbinden des Geräts an das Benutzerkonto, dem mithilfe des Administrationsservers ein entsprechendes Zertifikat zugewiesen wurde.

Es wird in diesem Fall die beidseitige SSL-Authentifizierung SSL (two-way SSL authentication, mutual authentication) verwendet. Sowohl der Administrationsserver als auch das Gerät werden mithilfe der Zertifikate authentifiziert.

Verbindung des Geräts ohne Benutzerzertifikat

Bei der Verbindung des Geräts ohne Benutzerzertifikat wird es nicht an ein Benutzerkonto auf dem Administrationsserver angebunden. Ruft das Gerät jedoch ein beliebiges Zertifikat ab, erfolgt ein Anbinden des Geräts an den Benutzer, dem das entsprechende Zertifikat mithilfe des Administrationsservers zugewiesen wurde.

Bei der Verbindung des Geräts mit dem Administrationsserver wird die einseitige SSL-Authentifizierung (one-way SSL authentication) verwendet, bei der nur der Administrationsserver mithilfe des Zertifikates authentifiziert wird. Nachdem das Gerät ein Benutzerzertifikat abgerufen hat, wird der Authentifizierungstyp auf beidseitige SSL-Authentifizierung (2-way SSL authentication, mutual authentication) geändert.

Anschlussschema für KES-Geräte mit dem Server unter Verwendung der erzwungenen Delegierung Kerberos (KCD)

Das Verbindungsschema für KES-Geräte zum Administrationsserver unter Verwendung von Kerberos Constrained Delegation (KCD) setzt voraus:

- Integration mit einem Reverse-Proxy, der KCD unterstützt.
- Nutzung von Kerberos Constrained Delegation (im Weiteren "KCD") zur Authentifizierung mobiler Geräte.
- Integration mit der Infrastruktur der offenen Schlüssel (Public Key Infrastructure, im Weiteren PKI) zur Verwendung von Benutzerzertifikaten.

Bei Verwendung dieses Verbindungsschemas muss Folgendes berücksichtigt werden:

- Der Verbindungstyp der KES-Geräte zum Reverse-Proxy muss "Zwei-Wege-SSL-Authentifizierung" sein. Das heißt, das Gerät muss gemäß seines proprietären Benutzerzertifikats mit dem Reverse-Proxy verbunden werden. Dazu muss im Installationspaket von Kaspersky Endpoint Security für Android, das auf dem Gerät installiert ist, das Benutzerzertifikat integriert sein. Dieses KES-Paket muss vom Administrationsserver speziell für das betreffende Gerät (den Benutzer) erstellt worden sein.
- Anstelle des Standardserverzertifikats muss für das mobile Protokoll ein besonderes (benutzerspezifisches) Zertifikat angegeben werden:

  1. Aktivieren Sie Im Eigenschaftenfenster des Administrationsservers im Abschnitt **Einstellungen** das Kontrollkästchen **Port für mobile Geräte öffnen**, wählen Sie in der Dropdown-Liste die Option **Zertifikat hinzufügen** aus.
  2. Geben Sie im folgenden Fenster dasselbe Zertifikat an, das auf dem Reverse-Proxy bei der Veröffentlichung des Zugriffspunkts für das mobile Protokoll auf dem Administrationsserver festgelegt wurde.

- Die Benutzerzertifikate für die KES-Geräte müssen von der Domänen-Certificate Authority (CA) ausgestellt werden. Beachten Sie dabei: Sollte die Domain mehrere Stamm-CAs beinhalten, müssen die Benutzerzertifikate mit jener CA ausgestellt werden, die bei der Veröffentlichung auf dem Reverse-proxy festgelegt wurde.

Die Übereinstimmung mit den Anforderungen des oben erwähnten Benutzerzertifikates kann auf verschiedene Weisen gewährleistet werden:

- Ein besonderes Benutzerzertifikat im Assistenten für das Erstellen von Installationspaketen und im Assistenten für die Installation eines Zertifikats angeben.
- Den Administrationsserver mit Domänen-PKI integrieren und die entsprechende Einstellung in den Regeln für die Ausstellung von Zertifikaten anpassen:

  1. Erweitern Sie die Konsolenstruktur im Ordner **Verwaltung mobiler Geräte** und wählen Sie den Unterordner **Zertifikate** aus.
  2. Öffnen Sie durch Klicken auf die Schaltfläche **Regeln für das Ausstellen von Zertifikaten anpassen** im Arbeitsbereich des Ordners **Zertifikate** das Fenster **Regeln für das Ausstellen von Zertifikaten**.
  3. Passen Sie im Abschnitt **PKI-Integration** die Integration mit der Public-Key-Infrastruktur an.
  4. Geben Sie im Abschnitt **Mobilgerät-Zertifikat ausstellen** die Quelle der Zertifikate an.

Als Beispiel dienen die Einstellungen für die eingeschränkte Delegierung von KCD mit den folgenden Annahmen:

- Der Zugriffspunkt auf das mobile Protokoll auf dem Administrationsserver liegt auf Port 13292.
- Der Name des Geräts mit dem Reverse-Proxy lautet "firewall.mydom.local".
- Der Gerätename mit dem Administrationsserver lautet ksc.mydom.local.
- Der Name der externen Veröffentlichung des Zugriffspunkts auf das mobile Protokoll lautet kes4mob.mydom.global.

Domänenbenutzerkonto für den Administrationsserver

Das Domänenbenutzerkonto (beispielsweise KSCMobileSrvcUsr), unter dem der Dienst des Administrationsservers ausgeführt werden soll, muss erstellt werden. Das Benutzerkonto für den Dienst des Administrationsservers kann bei der Installation des Administrationsservers oder mithilfe des Tools klsrvswch angegeben werden. Das Tool klsrvswch befindet sich im Installationsordner des Administrationsservers. Der Standardinstallationspfad lautet " <Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

Das Domänenbenutzerkonto muss aus folgenden Gründen angegeben werden:

- Die Funktionalität zur Verwaltung von KES-Geräten ist ein untrennbarer Bestandteil des Administrationsservers.
- Für die ordnungsgemäße Ausführung von Kerberos Constrained Delegation (KCD) muss die Empfängerseite (d. h. der Administrationsserver) unter einem Domänenbenutzerkonto ausgeführt werden.

Service Principal Name für http/kes4mob.mydom.local

In der Domäne unter dem Benutzerkonto KSCMobileSrvcUsr ist es erforderlich, den Service Principal Name (SPN) für die Veröffentlichung des Dienstes des mobilen Protokolls auf Port 13292 des Geräts mit dem Administrationsserver zu registrieren. Für das Gerät kes4mob.mydom.local mit dem Administrationsserver sieht dies folgendermaßen aus:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Konfigurieren der Domäneneigenschaften des Geräts mit dem Reverse-Proxy (firewall.mydom.local)

Für die Delegierung des Datenverkehres muss das Gerät mit dem Reverse-Proxy (firewall.mydom.local) jenem Dienst vertraut gemacht werden, der gemäß SPN festgelegt wurde (http/kes4mob.mydom.local:13292).

Um das Gerät mit dem Reverse-Proxy dem gemäß SPN bestimmten Dienst vertraut zu machen (http/kes4mob.mydom.local:13292), muss der Administrator wie folgt vorgehen:

1. Im dem Microsoft Management Console-Snap-in namens "Active Directory Users and Computers" muss das Gerät mit installiertem Reverse-Proxy (firewall.mydom.local) ausgewählt werden.

2. In den Eigenschaften des Geräts auf der Registerkarte **Delegation** für den Schalter **Trust this computer for delegation to specified service only**, die Variante **Use any authentication protocol** auswählen.

3. SPN http/kes4mob.mydom.local:13292 zur Liste **Services to which this account can present delegated credentials** hinzufügen.

Besonderes (benutzerspezifisches) Zertifikat für die Veröffentlichung (kes4mob.mydom.global)

Für die Veröffentlichung des mobilen Protokolls des Administrationsservers ist es erforderlich, ein besonderes (benutzerspezifisches) Zertifikat auf FQDN kes4mob.mydom.global auszustellen und es in der Verwaltungskonsole anstatt des Standardserverzertifikats in den Einstellungen des mobilen Protokolls des Administrationsservers anzugeben. Dazu muss im Eigenschaftenfenster des Administrationsservers im Abschnitt **Einstellungen** das Kontrollkästchen **Port für mobile Geräte öffnen** aktiviert und in der Dropdown-Liste die Option **Zertifikat hinzufügen** ausgewählt werden.

Es muss berücksichtigt werden, dass im Container mit dem Serverzertifikat (Datei mit der Erweiterung p12 oder pfx) auch die Kette der Stammzertifikate (öffentlichen Schlüssel) vorhanden sein muss.

Veröffentlichung auf dem Reverse-Proxy konfigurieren

Auf dem Reverse-Proxy muss für den Datenverkehr, der ausgehend von einem mobilen Gerät auf dem Port 139292 von kes4mob.mydom.global eingeht, die KCD auf dem SPN (http/kes4mob.mydom.local.13292) unter Verwendung des für den FQDN (kes4mob.mydom.global ausgestellten Zertifikats angepasst werden. Dabei muss berücksichtigt werden, dass sowohl bei der Veröffentlichung, als auch beim veröffentlichten Zugriffspunkt (Port 13292 des Administrationsservers) ein und dasselbe Serverzertifikat verwendet werden muss.

Verwendung von Firebase Cloud Messaging

Zur rechtzeitigen Zustellung von Befehlen auf KES-Geräten die durch das Android-Betriebssystem verwaltet werden, wird in Kaspersky Security Center das System der Push-Benachrichtigung verwendet. Push-Benachrichtigungen zwischen KES-Geräten und dem Administrationsserver werden mittels Firebase Cloud Messaging (im Folgenden als FCM bezeichnet) ausgetauscht. In der Kaspersky Security Center Verwaltungskonsole können Sie die Einstellungen für Firebase Cloud Messaging festlegen, um KES-Geräte an den Dienst anzuschließen.

Um die Einstellungen für Firebase Cloud Messaging zu erhalten, müssen Sie über ein Google-Benutzerkonto verfügen.

So aktivieren die Verwendung von FCM:

1. Wählen Sie in der Verwaltungskonsole zuerst den Knoten **Verwaltung mobiler Geräte** aus und dann den Ordner **Mobile Geräte**.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Mobile Geräte**, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie im Ordnereinstellungen den Abschnitt **Einstellungen von Firebase Cloud Messaging**.
4. Geben Sie im Feld **Firebase-Projektnummer** die ID des FCM Sender ein.
5. Wählen Sie im Feld **Datei mit privatem Schlüssel (JSON-Format)** die Datei mit dem privaten Schlüssel aus.

   Bei der nächsten Synchronisierung mit dem Administrationsserver werden KES-Geräte, die durch das Android-Betriebssystem verwaltet werden, an den Dienst Firebase Cloud Messaging angeschlossen.

Sie können die Einstellungen für Firebase Cloud Messaging mithilfe der Schaltfläche **Einstellungen zurücksetzen** ändern.

Wenn Sie zu einem anderen Firebase-Projekt wechseln, müssen Sie 10 Minuten warten, bis FCM fortgesetzt wird.

Der Dienst FCM arbeitet in den folgenden Adressbereichen:

- Seitens des KES-Gerätes ist der Zugriff auf die Ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) der folgenden Adressen erforderlich:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Alle IP-Adressen aus der Liste "Google ASN 15169"
- Seitens des Administrationsservers ist der Zugriff auf den Port 443 (HTTPS) der folgenden Adressen erforderlich:
  - fcm.googleapis.com
  - Oder auf allen IP aus der Liste "Google ASN 15169"

Falls in der Verwaltungskonsole in den Eigenschaften des Administrationsservers die Proxyserver-Einstellungen (**Erweitert** / **Einstellungen für den Internetzugriff konfigurieren**) festgelegt sind, werden sie für die Interaktion mit FCM verwendet.

Konfiguration von FCM: Datei mit der Sender ID und dem privaten Schlüssel abrufen

So konfigurieren Sie FCM:

1. Registrieren Sie sich auf dem Google-Portal.
2. Gehen Sie zur Firebase-Konsole.
3. Führen Sie eine der folgenden Aktionen aus:
   - Erstellen Sie ein neues Projekt, indem Sie auf **Projekt erstellen** klicken und den Anweisungen auf dem Bildschirm folgen.
   - Öffnen Sie ein vorhandenes Projekt.
4. Klicken Sie auf das Zahnrad-Symbol und wählen Sie **Projekteinstellungen** aus.

   Das Fenster **Projekteinstellungen** wird geöffnet.
5. Wählen Sie die Registerkarte **Cloud Messaging** aus.
6. Rufen Sie die relevante Sender-ID aus dem Feld **Sender ID** im Abschnitt **Firebase Cloud Messaging API (V1)** ab.
7. Wählen Sie die Registerkarte **Dienstkonten** aus und klicken Sie auf **Neuen privaten Schlüssel generieren**.
8. Klicken Sie im neuen Fenster auf **Schlüssel generieren**, um eine Datei mit einem privaten Schlüssel zu generieren und herunterzuladen.

Firebase Cloud Messaging ist jetzt konfiguriert.

Integration mit Public Key Infrastructure

Die Integration mit der Infrastruktur der offenen Schlüssel (Public Key Infrastructure, im Weiteren PKI) dient in erster Linie zur Vereinfachung der Ausstellung von Domänenbenutzerzertifikaten durch den Administrationsserver.

Der Administrator kann dem Benutzer in der Verwaltungskonsole ein Domänenzertifikat zuweisen. Dies kann auf eine der folgenden Weisen erfolgen:

- Dem Benutzer ein besonderes (benutzerspezifisches) Zertifikat aus der Datei im Assistenten für die Verbindung eines neuen Geräts oder im Assistenten für die Installation eines Zertifikats zuweisen.
- Eine Integration mit PKI ausführen und PKI als Quelle der Zertifikate für den konkreten Zertifikatstyp oder für alle Zertifikatstypen festlegen.

Die Einstellungen für die PKI-Integration werden im Arbeitsbereich des Ordners **Verwaltung mobiler Geräte** / **Zertifikate** verfügbar, indem Sie den Link **In Public-Key-Infrastruktur integrieren** anklicken.

Grundprinzip der PKI-Integration für die Ausstellung von Benutzerzertifikaten für Domänen

In der Verwaltungskonsole muss über den Link **In Public-Key-Infrastruktur integrieren** im Arbeitsbereich des Ordners **Verwaltung mobiler Geräte/Zertifikate** das Domänenbenutzerkonto festgelegt werden, das vom Administrationsserver für die Ausstellung von Domänenbenutzerzertifikaten mittels Domänen-CA verwendet wird (in Weiteren das Benutzerkonto, unter dem die PKI-Integration ausgeführt wird).

Dabei ist muss Folgendes berücksichtigt werden:

- In den Einstellungen der PKI-Integration gibt es die Möglichkeit, eine Standardvorlage für alle Zertifikatstypen anzugeben. In den Regeln für das Ausstellen von Zertifikaten (die Regeln sind im Arbeitsbereich des Ordners **Verwaltung mobiler Geräte/Zertifikate** mithilfe der Schaltfläche **Regeln für das Ausstellen von Zertifikaten anpassen** verfügbar) besteht hingegen die Möglichkeit, die Vorlage für jeden Typ des Zertifikates separat festzulegen.

- Auf dem Gerät mit dem installierten Administrationsserver muss im Zertifikatsspeicher des Benutzerkontos, unter dem die PKI-Integration ausgeführt wird, das Spezialzertifikat Enrollment Agent (EA) installiert sein. Das Zertifikat Enrollment Agent (EA) wird vom Administrator der Domänen-CA (Certificate Authority) ausgestellt.

Das Benutzerkonto, unter dem die PKI-Integration ausgeführt wird, muss den folgenden Kriterien entsprechen:

- Ist Domänenbenutzer.

- Ist lokaler Administrator des Geräts mit dem installierten Administrationsserver, von dem die PKI-Integration ausgeführt wird.

- Verfügt über die Berechtigung *Als Dienst anmelden*.

- Unter diesem Benutzerkonto muss zumindest einmal das Gerät mit dem installierten Administrationsserver gestartet werden, um ein ständiges Benutzerprofil zu erstellen.

Kaspersky Security Center Webserver

Der Kaspersky Security Center Webserver (Im Weiteren der Webserver) ist eine Komponente von Kaspersky Security Center. Der Webserver dient zur Veröffentlichung von autonomen Installationspaketen, autonomen Installationspaketen für mobile Geräte sowie Dateien aus dem freigegebenen Ordner.

Die erstellten Installationspakete werden automatisch auf dem Webserver veröffentlicht und nach dem ersten Download gelöscht. Der Administrator kann den erstellten Link auf beliebige Weise an den Benutzer übermitteln, z. B. per E-Mail.

Über diesem Link kann der Benutzer die für erforderlichen Informationen auf ein mobiles Gerät herunterladen.

Webserver-Einstellungen

Wenn Sie den Webserver noch genauer anpassen möchten, können Sie in den Webserver-Eigenschaften die Ports für die Protokolle HTTP (8060) und HTTPS (8061) ändern. Ferner ist neben dem Wechsel der Ports der Wechsel des Serverzertifikats für das HTTPS-Protokoll und der Wechsel des FQDN-Namens des Webservers für das HTTP-Protokoll möglich.

Weitere Routinearbeiten

Dieser Abschnitt enthält Empfehlungen für die tägliche Arbeit mit Kaspersky Security Center.

Farbliche Kennzeichnungen und protokollierte Ereignissen in der Verwaltungskonsole überwachen

Mithilfe der farblichen Kennzeichnungen kann der aktuelle Status von Kaspersky Security Center und der verwalteten Geräte in der Verwaltungskonsole rasch bewertet werden. Die Kennzeichnungen werden im Arbeitsbereich des Knotens **Administrationsserver** auf der Registerkarte **Überwachung** angezeigt. Auf der Registerkarte gibt es sechs Informationsbereiche mit farblichen Kennzeichnungen und protokollierten Ereignissen. Die farbliche Kennzeichnung besteht aus einer farbigen vertikalen Leiste auf der linken Seite des Bereichs. Jeder Block mit Kennzeichnung steht für einen separaten funktionalen Bereich von Kaspersky Security Center (s. Tabelle unten).

Zuständigkeitsbereiche der farblichen Kennzeichnungen in der Verwaltungskonsole

Bereichsname	Zuständigkeitsbereich der farblichen Kennzeichnung
Bereitstellung	Installation des Administrationsagenten und der Sicherheitsanwendungen auf den Geräten im Unternehmensnetzwerk
Verwaltungsstruktur	Struktur der Administrationsgruppen. Scannen des Netzwerkes. Verschiebungsregeln für Geräte
Schutzeinstellungen	Funktionen der Sicherheitsanwendung: Schutzstatus, Schadsoftware-Untersuchung
Update	Updates und Patches
Überwachung	Schutzstatus
Administrationsserver	Funktionen und Eigenschaften des Administrationsservers

Die Kennzeichnung kann eine von fünf Farben aufweisen (s. Tabelle unten). Die Farbe der Kennzeichnung hängt vom aktuellen Status von Kaspersky Security Center und den registrierten Ereignissen ab.

Farbkodierung der Kennzeichnungen

Status	Farbe der Kennzeichnung	Farbwert der Kennzeichnung
Informativ	Grün	Keine Aktion des Administrators erforderlich.
Warnung	Gelb	Es ist eine Aktion des Administrators erforderlich.
Kritisch	Rot	Es gibt ernste Probleme. Für deren Behebung ist eine Aktion des Administrators erforderlich.
Informativ	Blau	Es sind Ereignisse registriert, die nicht mit potentiellen oder tatsächlichen Bedrohungen für die Sicherheit der verwalteten Geräte verbunden sind.
Informativ	Grau	Keine Informationen über die Ereignisse verfügbar oder noch keine Informationen erhalten.

Der Administrator sollte dafür sorgen, dass die Farbkennzeichnung aller Informationsbereiche auf der Registerkarte **Überwachung** grün bleibt.

In den Informationsbereichen werden auch protokollierte Ereignisse angezeigt, die sich auf die Farbkennzeichnungen und den Status von Kaspersky Security Center auswirken (siehe Tabelle unten).

Name, Beschreibung und farbliche Kennzeichnung der protokollierten Ereignisse

Farbe der Kennzeichnung	Dargestellter Name des Ereignistyps	Ereignistyp	Beschreibung
Rot	**Lizenz ist auf %1 Gerät(en) abgelaufen**	IDS_AK_STATUS_LIC_EXPAIRED	Ereignisse dieser Art treten auf, wenn der Gültigkeitszeitraum einer kommerziellen Lizenz abgelaufen ist. Kaspersky Security Center prüft einmal täglich, ob die Lizenz auf den Geräten abgelaufen ist. Wenn die kommerzielle Lizenz abläuft, stellt Kaspersky Security Center nur grundlegende Funktionen bereit. Um Kaspersky Security Center weiter Verwenden zu können, müssen Sie die kommerziellen Lizenz verlängern.
Rot	**Die Sicherheitsanwendung wurde nicht gestartet auf: %1 Gerät(en)**	IDS_AK_STATUS_AV_NOT_RUNNING	Ereignisse dieser Art treten auf, wenn die auf dem Gerät installierte Sicherheitsanwendung nicht ausgeführt wird. Stellen Sie sicher, dass Kaspersky Endpoint Security auf dem Gerät ausgeführt wird.
Rot	**Schutz nicht gestartet auf: %1 Gerät(en)**	IDS_AK_STATUS_RTP_NOT_RUNNING	Ereignisse dieser Art treten auf, wenn die Sicherheitsanwendung auf dem Gerät länger deaktiviert war, als per festgelegtem Zeitintervall erlaubt. Überprüfen Sie den aktuellen Status des Echtzeitschutzes auf dem Gerät und stellen Sie sicher, dass alle benötigten Schutzkomponenten aktiviert sind.
Rot	**Auf den Geräten wurde eine Schwachstelle in Programmen gefunden**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Ereignisse dieser Art treten auf, wenn die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* auf dem Gerät Schwachstellen mit der Signifikanz gefunden hat, die in den installierten Programmen auf dem Gerät angegeben wurde Prüfen Sie die Liste der verfügbaren Updates im Unterordner **Programm-Updates**, der sich im Ordner **Programmverwaltung** befindet. Dieser Ordner enthält eine Liste der durch den Administrationsserver heruntergeladenen Updates für Microsoft-Programme und Programme anderer Softwarehersteller, die auf Geräte verteilt werden können. Nachdem Sie die Informationen über die verfügbaren Updates geprüft haben, installieren Sie die Updates auf den Geräten.
Rot	**Auf dem Administrationsserver wurden kritische Ereignisse registriert**	IDS_AK_STATUS_EVENTS_OCCURED	Ereignisse dieser Art treten auf, wenn kritische Ereignisse des Administrationsservers erkannt werden. Überprüfen Sie die Liste Ereignisse, die auf dem Administrationsserver gespeichert ist, und korrigieren Sie die kritischen Ereignisse nacheinander.
Rot	**Es wurden Fehler in Ereignissen auf dem Administrationsserver protokolliert**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Ereignisse dieser Art treten auf, wenn auf der Seite des Administrationsservers unerwartete Fehler protokolliert werden. Überprüfen Sie die Liste Ereignisse, die auf dem Administrationsserver gespeichert ist, und korrigieren Sie die Fehler-Ereignisse nacheinander.

Farbe der Kennzeichnung	Dargestellter Name des Ereignistyps	Ereignistyp	Beschreibung
Rot	**Verbindung mit %1 Gerät(en) wurde unterbrochen**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Ereignisse dieser Art treten auf, wenn die Verbindung zwischen dem Administrationsserver und dem Gerät unterbrochen wird. Zeigen Sie die Liste mit den nicht verbundenen Geräten an und versuchen Sie, diese erneut zu verbinden.
Rot	**Der Administrationsserver hatte seit Langem keine Verbindung zu %1 Gerät(en)**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Ereignisse dieser Art treten auf, wenn sich das Gerät innerhalb des festgelegten Zeitraums nicht mit dem Administrationsserver verbunden hat, da das Gerät ausgeschaltet war. Stellen Sie sicher, dass das Gerät eingeschaltet ist und der Administrationsagent auf ihm ausgeführt wird.
Rot	**%1 Gerät(e) ohne Status OK**	IDS_AK_STATUS_HOST_NOT_OK	Ereignisse dieser Art treten auf, wenn sich der Status *OK* des mit dem Administrationsserver verbundenen Geräts in *Kritisch* oder *Warnung* ändert. Sie können das Problem mithilfe des Tools zur Ferndiagnose von Kaspersky Security Center beheben.
Rot	**Datenbanken sind veraltet auf: %1 Gerät(en)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Ereignisse dieser Art treten auf, wenn die Antiviren-Datenbanken auf dem Gerät nicht innerhalb des festgelegten Zeitraums aktualisiert wurden. Folgen Sie den Anweisungen, um die Kaspersky-Datenbanken zu aktualisieren.
Rot	**Gerät(e) mit lange nicht ausgeführter Suche nach Windows-Updates: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Ereignisse dieser Art treten auf, wenn die Aufgabe *Windows-Updates synchronisieren* nicht innerhalb des angegebenen Zeitintervalls ausgeführt wurde. Folgen Sie den Anweisungen, um Updates von Windows Update mit dem Administrationsserver zu synchronisieren.
Rot	**Die Installation von %1 Plug-in(s) für Kaspersky Security Center ist erforderlich**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Ereignisse dieser Art treten auf, wenn Sie zusätzliche Plug-ins für Kaspersky-Anwendungen installieren müssen. Laden Sie die erforderlichen Verwaltungs-Plug-ins für die Kaspersky-Anwendung von der Webseite des Technischen Supports von Kaspersky herunter und installieren Sie sie.

Remote-Zugriff auf verwaltete Geräte

Dieser Abschnitt enthält Informationen über den Remote-Zugriff auf verwaltete Geräte.

Verwenden der Option "Verbindung mit Administrationsserver nicht trennen" zur Bereitstellung einer dauerhaften Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver

Wenn Sie keine Push-Server verwenden, bietet Kaspersky Security Center keine kontinuierliche Verbindung zwischen verwalteten Geräten und dem Administrationsserver. Die Administrationsagenten auf den verwalteten Geräten stellen regelmäßig eine Verbindung mit dem Administrationsserver her und führen eine Synchronisierung durch. Die Dauer des Zeitraums einer solcher Synchronisierung wird in der Richtlinie des Administrationsagenten festgelegt. Wenn eine frühzeitige Synchronisierung erforderlich ist, sendet der Administrationsserver (oder ein Verteilungspunkt, falls verwendetet) ein signiertes Netzwerkpaket über ein IPv4- oder IPv6-Netzwerk an den UDP-Port des Administrationsagenten. Standardmäßig wird Port 15000 verwendet. Wenn über UDP keine Verbindung vom Administrationsserver zum verwalteten Gerät möglich ist, wird die Synchronisierung bei der nächsten routinemäßigen Verbindung des Administrationsagenten mit dem Administrationsserver im Laufe des Synchronisierungsintervalls durchgeführt.

Einige Vorgänge können ohne eine frühzeitige Verbindung zwischen dem Administrationsagenten und dem Administrationsserver nicht ausgeführt werden, wie z. B. das Starten und Stoppen lokaler Aufgaben, das Empfangen von Statistiken für eine verwaltetes Programm oder das Herstellen eines Tunnels. Um dieses Problem für den Fall zu beheben, dass Sie keine Push-Server verwenden, können Sie die Option **Verbindung mit Administrationsserver nicht trennen** verwenden, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht.

So stellen Sie eine dauerhafte Verbindung zwischen einem Client-Gerät und dem Administrationsserver bereit:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
2. Wählen Sie im Arbeitsbereich des Ordners das verwaltete Gerät aus, mit dem Sie eine dauerhafte Verbindung bereitstellen möchten.
3. Wählen Sie im Kontextmenü des Geräts den Punkt **Eigenschaften** aus.

   Das Eigenschaftenfenster des gewählten Geräts wird geöffnet.
4. Wählen Sie im Abschnitt **Allgemein** des angezeigten Fensters die Option **Verbindung mit Administrationsserver nicht trennen**.

Zwischen dem verwalteten Gerät und Administrationsserver wurde eine dauerhafte Verbindung hergestellt.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

Über das Überprüfen der Verbindungszeit des Geräts mit dem Administrationsserver

Wenn ein Gerät heruntergefahren wird, benachrichtigt der Administrationsagent den Administrationsserver über dieses Ereignis. In der Verwaltungskonsole wird das Gerät als heruntergefahren angezeigt. Der Administrationsagent kann den Administrationsserver jedoch nicht über alle derartigen Ereignisse benachrichtigen. Der Administrationsserver analysiert deshalb periodisch das Attribut **Verbindung mit dem Administrationsserver** (Dieser Wert des Attributs wird in der Verwaltungskonsole in den Geräteeigenschaften im Abschnitt **Allgemein** angezeigt) für jedes Gerät und vergleicht es mit dem Synchronisierungsintervall aus den aktuellen Einstellungen des Administrationsagenten. Wenn ein Gerät über mehr als drei aufeinander folgende Synchronisationsintervalle nicht reagiert hat, wird dieses Gerät als abgeschaltet markiert.

Über erzwungene Synchronisierung

Obwohl Kaspersky Security Center den Status, die Einstellungen, die Aufgaben und die Richtlinien für die verwalteten Geräte automatisch synchronisiert, muss der Administrator in einzelnen Fällen genau wissen, ob an diesem Moment für ein bestimmtes Gerät die Synchronisierung ausgeführt worden ist.

Das Kontextmenü der verwalteten Geräte in der Verwaltungskonsole enthält im Menüpunkt **Alle Aufgaben** den Befehl **Synchronisierung erzwingen**. Wenn Kaspersky Security Center 15.1 diesen Befehl ausführt, versucht der Administrationsserver, eine Verbindung zum Gerät herzustellen. Ist dieser Versuch erfolgreich, so wird die Synchronisierung erzwungen. Andernfalls erfolgt die erzwungene Synchronisierung erst nach der nächsten geplanten Verbindung des Administrationsagenten mit dem Administrationsserver.

Über das Tunneln von Verbindungen

Kaspersky Security Center erlaubt das Tunneln der TCP-Verbindungen von der Verwaltungskonsole über den Administrationsserver und weiter über den Administrationsagenten zum angegebene Port auf dem verwalteten Gerät. Das Tunneln wird für den Fall, dass eine direkte Verbindung des Geräts mit der Verwaltungskonsole unmöglich ist, für die Verbindung des Client-Programms, welches sich auf dem Gerät mit der installierten Verwaltungskonsole befindet, zum TCP-Port des verwalteten Gerät verwendet.

Insbesondere wird das Tunneln für die Remotedesktopverbindung verwendet: sowohl für die Verbindung mit einer bestehenden Sitzung, als auch für das Erstellen einer neuen Remote-Sitzung.

Ferner kann das Tunneln mithilfe von externen Tools verwendet werden. Insbesondere kann der Administrator so das Tool putty, den VNC-Client und weitere Tools starten.

Handbuch zur Skalierung

Dieser Abschnitt enthält Informationen über die Skalierung von Kaspersky Security Center.

Zu diesem Handbuch

Das Handbuch zur Skalierung von Kaspersky Security Center 15.1 (auch als "Kaspersky Security Center" bezeichnet) richtet sich an Experten, die für die Installation und Administration von Kaspersky Security Center zuständig sind, sowie an Experten, die für den technischen Support von Unternehmen verantwortlich sind, die Kaspersky Security Center einsetzen.

Alle Empfehlungen und Berechnungen sind für Netzwerke vorgesehen, in denen Kaspersky Security Center den Schutz von Geräten mit installierter Software von Kaspersky verwaltet (dazu gehören auch mobile Geräte). Wenn mobile Geräte oder andere verwaltete Geräte separat betrachtet werden sollen, wird dies ausdrücklich erwähnt.

Zur Erreichung und Aufrechterhaltung der optimalen Leistung unter verschiedenen Arbeitsbedingungen berücksichtigen Sie die Anzahl der Geräte im Netzwerk, die Netztopologie und den erforderlichen Funktionsumfang von Kaspersky Security Center.

Das Handbuch enthält folgende Informationen:

- Einschränkungen von Kaspersky Security Center
- Berechnungen für die wichtigsten Nodes von Kaspersky Security Center (Administrationsserver und Verteilungspunkte):
    - Hardwarevoraussetzungen für die Administrationsserver und Verteilungspunkte
    - Berechnung der Anzahl und der Hierarchie der Administrationsserver
    - Berechnung der Anzahl und der Konfiguration der Verteilungspunkte
- Konfiguration der Speicherung von Ereignissen in der Datenbank in Abhängigkeit von der Anzahl der Geräte im Netzwerk
- Bewährte Methoden zur Optimierung der Leistungs
- Konfiguration bestimmter Aufgaben, welche die optimale Leistung von Kaspersky Security Center gewährleisten
- Verbrauch von Datenverkehr (Netzwerkbelastung) zwischen dem Kaspersky Security Center Administrationsserver und jedem geschützten Gerät

Es wird empfohlen, dieses Handbuch in den folgenden Situationen zu konsultieren:

- Wenn Sie vor der Installation von Kaspersky Security Center die Verteilung von Ressourcen planen.
- Wenn Sie die Größe des Netzwerks wesentlich ändern möchten, in dem Kaspersky Security Center bereitgestellt wurde.

- Wenn Sie Kaspersky Security Center bisher innerhalb eines begrenzten Netzwerksegments (in einer Testumgebung) verwendet haben und jetzt zur vollständigen Bereitstellung von Kaspersky Security Center im Unternehmensnetzwerk wechseln.

- Bei Änderungen in der Auswahl der verwendeten Funktionen von Kaspersky Security Center.

Informationen zu Einschränkungen von Kaspersky Security Center

In der nachfolgenden Tabelle sind die Einschränkungen der aktuellen Version von Kaspersky Security Center aufgelistet.

Einschränkungen von Kaspersky Security Center

Typ der Einschränkung	Wert
Maximale Anzahl verwalteter Geräte eines Administrationsservers	100.000
Maximale Anzahl von Geräte mit aktivierter Option **Verbindung mit Administrationsserver nicht trennen**	300
Maximale Anzahl von Administrationsgruppen	10.000
Maximale Anzahl gespeicherter Ereignisse	45.000.000
Maximale Anzahl von Richtlinien	2.000
Maximale Anzahl von Aufgaben	2.000
Maximale Gesamtanzahl von Active Directory-Objekten (Organisationseinheiten (OU) und Benutzerkonten, Geräte und Sicherheitsgruppen)	1.000.000
Maximale Anzahl der Profile in der Richtlinie	100
Maximale Anzahl der sekundären Administrationsserver bei einem primären Administrationsserver	500
Maximale Anzahl der virtuellen Administrationsserver	500
Maximale Anzahl der Geräte, die ein einzelner Verteilungspunkt abdecken kann (Verteilungspunkte können nur nicht-mobile Geräte abdecken)	10.000
Maximale Anzahl der Geräte, die ein einzelnes Verbindungs-Gateway verwenden können	10.000, inklusive mobile Geräte
Maximale Anzahl der mobilen Geräte, die ein einziger Administrationsserver verwalten kann	100.000, abzüglich der Anzahl der stationären verwalteten Geräte

Berechnungen für die Administrationsserver

Dieser Abschnitt enthält die Software- und Hardwareanforderungen für Geräte, die als Administrationsserver verwendet werden. Ferner werden Empfehlungen für die Berechnung der Anzahl und für die Hierarchie von Administrationsservern abhängig von der Konfiguration des Unternehmensnetzwerks bereitgestellt.

Berechnung von Hardwareressourcen für den Administrationsserver

Dieser Abschnitt enthält Berechnungen, die bei der Planung der Hardwareressourcen für den Administrationsserver verwendet werden können. Zusätzlich wird eine Empfehlung hinsichtlich der Berechnung des Speicherplatzes auf dem Laufwerk angebracht, der bei Verwendung der Funktionalität Schwachstellen- und Patch-Management benötigt wird.

Hardwarevoraussetzungen für DBMS und Administrationsserver

Die nachfolgenden Tabellen zeigen die empfohlenen, anhand eines Tests ermittelten, minimalen Hardwarevoraussetzungen für das DBMS und den Administrationsserver. Die vollständige Liste mit unterstützten Betriebssystemen und DBMS finden Sie bei den Hard- und Softwarevoraussetzungen.

Administrationsserver und DBMS befinden sich auf verschiedenen Geräten, das Netzwerk umfasst 50.000 Geräte

Konfiguration des Geräts mit dem Administrationsserver

Hardware	Wert
Prozessor	4 Kerne, 2500 MHz
Arbeitsspeicher	8 GB
Festplatte	300 GB, RAID empfohlen
Netzwerkadapter	1 Gbit

Konfiguration des Geräts mit installiertem DBMS

Hardware	Wert
Prozessor	4 Kerne, 2500 MHz
Arbeitsspeicher	16 GB
Festplatte	200 GB SATA RAID
Netzwerkadapter	1 Gbit

Administrationsserver und DBMS befinden sich auf demselben Gerät, das Netzwerk umfasst 50.000 Geräte

Konfiguration des Geräts mit installiertem Administrationsserver und DBMS

Hardware	Wert
Prozessor	8 Kerne, 2500 MHz
Arbeitsspeicher	16 GB
Festplatte	500 GB SATA RAID
Netzwerkadapter	1 Gbit

Administrationsserver und DBMS befinden sich auf verschiedenen Geräten, das Netzwerk umfasst 100.000 Geräte

Konfiguration des Geräts mit dem Administrationsserver

Hardware	Wert
Prozessor	8 Kerne, 2,13 GHz
Arbeitsspeicher	8 GB
Festplatte	1 TB, RAID
Netzwerkadapter	1 Gbit

Konfiguration des Geräts mit installiertem DBMS

Hardware	Wert
Prozessor	8 Kerne, 2,53 GHz
Arbeitsspeicher	26 GB
Festplatte	500 GB SATA RAID
Netzwerkadapter	1 Gbit

Die Tests wurden mit den folgenden Einstellungen durchgeführt:

- Auf dem Administrationsserver ist die automatische Bestimmung von Verteilungspunkten aktiviert oder die Verteilungspunkte werden manuell gemäß der empfohlenen Tabelle bestimmt
- Die Aufgabe zum Verschieben ins Backup speichert die Backup-Kopien in der Dateiressource, die sich auf einem separaten Server befindet
- Der Zeitraum der Synchronisierung der Administrationsagenten ist entsprechend der nachfolgenden Tabelle konfiguriert.

  Synchronisierungsintervall der Administrationsagenten

Synchronisierungsintervall, Minute	Anzahl der verwalteten Geräte
15	10.000
30	20.000
45	30.000
60	40.000
75	50.000
150	100.000

Berechnung des Speicherplatzes in der Datenbank

Der Speicherplatz, der von der Datenbank belegt wird, kann näherungsweise mit folgender Formel berechnet werden:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

wobei:

- "C" – Anzahl der Geräte.
- "E" – Anzahl der gespeicherten Ereignisse.

- "A" – Gesamtsumme der Active Directory-Objekte:
  - Benutzerkonten der Geräte
  - Benutzerkonten
  - Benutzerkonten der Sicherheitsgruppen
  - Unterverzeichnisse von Active Directory

  Wenn die Abfrage von Active Directory deaktiviert ist, dann muss der Wert "A" mit Null angenommen werden.
- N ist die durchschnittliche Anzahl inventarisierter ausführbarer Dateien auf einem Endpunktgerät.
- F ist die Anzahl der Endpunktegeräte, auf denen ausführbare Dateien inventarisiert wurden.

Wenn Sie in den Einstellungen der Richtlinie für Kaspersky Endpoint Security die Übermittlung von Informationen über die ausgeführten Programme an den Administrationsserver aktivieren möchten, werden für die Speicherung der Informationen über die ausgeführten Programme weitere (0,03 * C) GB benötigt.

Wenn Windows-Updates über den Administrationsserver verteilt werden (Rolle eines WSUS-Servers), werden in der Datenbank zusätzlich 2,5 GB benötigt.

Während der Ausführung bildet sich in der Datenbank immer ein sogenannter *nicht benutzter Speicherplatz* (unallocated space). Daher ist die tatsächliche Dateigröße der Datenbank (standardmäßig die Datei KAV.mdf im Fall der Verwendung des Datenbankverwaltungssystems "SQL Server") häufig ungefähr doppelt so groß wie der in der Datenbank benutzte Speicherplatz.

Es wird davon abgeraten, die Größe des Transportprotokolls explizit einzuschränken (standardmäßig die Datei KAV_log.LDF, falls das DBMS "SQL Server" verwendet wird). Behalten Sie den Standardwert des Parameters MAXSIZE bei. Wenn Sie jedoch die Größe dieser Datei begrenzen müssen, berücksichtigen Sie dabei, dass der üblicherweise erforderliche minimale Wert des Parameters MAXSIZE für KAV_log.LDF 20480 MB beträgt.

Berechnung des Speicherplatzes auf dem Laufwerk (mit und ohne Berücksichtigung der Verwendung von Schwachstellen- und Patch-Management)

Berechnung des Speicherplatzes auf dem Laufwerk ohne Berücksichtigung der Verwendung von Schwachstellen- und Patch-Management

Der Speicherplatz auf dem Laufwerk des Administrationsservers, den das Verzeichnis %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit benötigt, kann anhand folgender Formel ungefähr berechnet werden:

(724 * C + 0,15 * E + 0,17 * A), KB

wobei:

- "C" – Anzahl der Geräte.
- "E" – Anzahl der gespeicherten Ereignisse.

- "A" – Gesamtsumme der Active Directory-Objekte:
  - Benutzerkonten der Geräte
  - Benutzerkonten
  - Benutzerkonten der Sicherheitsgruppen
  - Unterverzeichnisse von Active Directory

Wenn die Abfrage von Active Directory deaktiviert ist, dann muss der Wert "A" mit Null angenommen werden.

Berechnung des zusätzlichen Speicherplatzes auf dem Laufwerk unter Berücksichtigung der Verwendung von Schwachstellen- und Patch-Management

- Updates. Im gemeinsamen Ordner sind zusätzlich mindestens 4 GB zur Speicherung der Updates erforderlich.
- Installationspakete. Wenn auf dem Administrationsserver im gemeinsamen Ordner Installationspakete vorhanden sind, wird zusätzlicher Speicherplatz benötigt, welcher der Gesamtgröße der vorhandenen Installationspakete entspricht.
- Aufgaben zur Remote-Installation. Wenn auf dem Administrationsserver Aufgaben zur Remote-Installation vorhanden sind, ist auf dem Laufwerk zusätzlicher Speicherplatz (im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) in der Größe erforderlich, die der Summe aller zu installierenden Installationspakete entspricht.
- Patches. Wenn der Administrationsserver für die Installation von Patches verwendet wird, besteht erweiterter Platzbedarf auf dem Laufwerk:
  - Im Ordner für die Speicherung der Patches entspricht die Größe des Speicherplatzes der Gesamtgröße aller heruntergeladenen Patches. Standardmäßig werden Patches im Ordner "%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles" gespeichert.

    Mit dem Tool "klsrvswch" können Sie einen anderen Ordner zum Speichern von Patches angeben. Das Tool "klsrvswch" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "<Laufwerksbuchstabe>:\Programme (x86)\ Kaspersky Lab\ Kaspersky Security Center".

    Wenn der Administrationsserver als WSUS verwendet wird, ist es empfehlenswert, unter diesen Ordner mindestens 100 GB zu reservieren.
  - Im Verzeichnis %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit entspricht die Größe des Speicherplatzes der Gesamtgröße der Patches, auf welche die vorhandenen Exemplare der Aufgaben zur Installation von Updates (Patches) und zum Schließen von Schwachstellen verweisen.

Berechnung der Anzahl und der Konfiguration der Administrationsserver

Um die Auslastung des primären Administrationsservers zu verringern, können Sie jeder Administrationsgruppe einen separaten Administrationsserver zuweisen. Die Anzahl der sekundären Administrationsserver eines primären Administrationsservers darf höchstens 500 betragen.

Es wird empfohlen, bei der Konfiguration der Administrationsserver die Struktur Ihres Unternehmensnetzwerks zu berücksichtigen.

Empfehlungen für die Verbindung dynamischer virtueller Maschinen mit Kaspersky Security Center

Dynamische virtuelle Maschinen (auch als dynamische VMs bezeichnet) verbrauchen mehr Ressourcen als statische virtuelle Maschinen.

Weitere Informationen zu dynamischen virtuellen Maschinen finden Sie unter Unterstützung dynamischer virtueller Maschinen.

Wenn eine neue dynamische VM verbunden wird, erstellt Kaspersky Security Center ein Symbol für diese dynamische VM in der Verwaltungskonsole und verschiebt die dynamische VM in die Administrationsgruppe. Anschließend wird die dynamische VM zur Datenbank des Administrationsservers hinzugefügt. Der Administrationsserver wird vollständig mit dem Administrationsagenten synchronisiert, der auf dieser dynamischen VM installiert ist.

Im Netzwerk einer Organisation erstellt der Administrationsagent die folgenden Netzwerklisten für jede dynamische VM:

- Hardware
- Installierte Software
- Erkannte Schwachstellen
- Ereignisse und Listen von ausführbaren Dateien der Komponente "Programmkontrolle"

Der Administrationsagent überträgt diese Netzwerklisten an den Administrationsserver. Die Größe der Netzwerklisten hängt von den auf der dynamischen VM installierten Komponenten ab und kann die Leistung von Kaspersky Security Center und Datenbankverwaltungssystems (DBMS) beeinträchtigen. Beachten Sie, dass die Belastung nichtlinear wachsen kann.

Nachdem der Benutzer die Arbeit mit der dynamischen VM beendet und sie ausgeschaltet hat, wird diese Maschine aus der virtuellen Infrastruktur entfernt und Einträge zu dieser Maschine werden aus der Administrationsserver-Datenbank entfernt.

All diese Aktionen verbrauchen viele Datenbankressourcen von Kaspersky Security Center und dem Administrationsserver und können die Leistung von Kaspersky Security Center und des DBMS beeinträchtigen. Wir empfehlen, dass Sie bis zu 20.000 dynamische VMs mit Kaspersky Security Center zu verbinden.

Sie können mehr als 20.000 dynamische VMs mit Kaspersky Security Center verbinden, wenn die verbundenen dynamischen VMs Standardvorgänge ausführen (z. B. Datenbankaktualisierungen) und nicht mehr als 80% des Arbeitsspeichers und 75–80% der verfügbaren Kerne verbrauchen.

Das Ändern von Richtlinieneinstellungen, Programmen oder Betriebssystemen auf den dynamischen VMs kann den Ressourcenverbrauch verringern oder erhöhen. Als optimal gilt ein Verbrauch von 80–95% der Ressourcen.

Berechnungen für Verteilungspunkte und Verbindungs-Gateways

Dieser Abschnitt enthält die Hardwarevoraussetzungen für die Geräte, die als Verteilungspunkte verwendet werden, sowie Empfehlungen zur Berechnung der Anzahl von Verteilungspunkten und Verbindungs-Gateways in Abhängigkeit von der Struktur des Unternehmensnetzwerks.

Voraussetzungen für Verteilungspunkte

Für die Verwaltung von bis zu 10.000 Client-Geräten muss ein Verteilungspunkt die folgenden Mindestanforderungen erfüllen (eine Testkonfiguration wird bereitgestellt):

- CPU: Intel® Core™ i7-7700 CPU, 3.60 GHz mit 4 Prozessorkernen.
- RAM: 8 GB.
- Freier Speicherplatz: 120 GB.

Es wird nicht empfohlen, den Administrationsserver als Verteilungspunkt zuzuweisen, da dies die Belastung des Administrationsservers erhöht.

Wenn auf dem Administrationsserver Aufgaben zur Remote-Installation vorhanden sind, ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher Speicherplatz in der Größe erforderlich, die der Summe aller zu installierenden Installationspakete entspricht.

Wenn auf dem Administrationsserver ein oder mehrere Instanzen einer Aufgabe zur Installation von Updates (Patches) und zum Schließen von Schwachstellen vorhanden sind, ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher Speicherplatz in der Größe erforderlich, die der doppelten Summe aller zu installierenden Patches erforderlich.

Bei Verwendung des Schemas, bei dem die Verteilungspunkte die Datenbanken-Updates und Programm-Module direkt von den Kaspersky-Update-Servern abrufen, müssen die Verteilungspunkte mit dem Internet verbunden sein.

Anzahl und Konfiguration der Verteilungspunkte bestimmen

Je mehr Client-Geräte ein Netzwerk enthält, desto mehr Verteilungspunkte sind erforderlich. Es wird empfohlen, die automatische Zuweisung von Verteilungspunkten nicht zu deaktivieren. Bei aktivierter automatischer Zuweisung der Verteilungspunkte weist der Administrationsserver bei einer großen Anzahl an Client-Geräten automatisch Verteilungspunkte zu und bestimmt ihre Konfiguration.

Verwendung exklusiv zugewiesener Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte eine Reihe von bestimmten Geräten zu verwenden (d. h., exklusiv zugewiesene Server), so können Sie auf die automatische Zuweisung der Verteilungspunkte verzichten. Überzeugen Sie sich in diesem Fall davon, dass die Geräte, die Sie zu Verteilungspunkten bestimmen möchten, über ausreichend freien Speicherplatz auf dem Datenträger verfügen, nicht regelmäßig abgeschaltet werden und dass auf ihnen der Ruhezustand deaktiviert ist.

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–100	1
Über 100	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Verwendung von Standard-Client-Geräten (Workstations) als Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte Standard-Client-Geräte (d. h., Workstations) zu verwenden, wird zur Vermeidung einer unnötigen Belastung des Administrationsservers empfohlen, die Verteilungspunkte auf folgende Weise zuzuweisen (s. nachfolgende Tabelle):

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–30	1
31–300	2
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Wenn ein Verteilungspunkt abgeschaltet (oder aus anderen Gründen nicht verfügbar) ist, können die verwalteten Geräte in seinem Bereich Updates vom Administrationsserver abrufen.

Berechnung der Anzahl der Verbindungs-Gateways

Wenn Sie ein Verbindungs-Gateway verwenden möchten, wird empfohlen, ein Gerät speziell für diesen Zweck zu bestimmen.

Ein Verbindungs-Gateway kann maximal 10.000 verwaltete Geräte einschließlich mobilen Geräten abdecken.

Speicherung der Daten zu Ereignissen für Aufgaben und Richtlinien

Dieser Abschnitt enthält Berechnungen, die sich auf die Speicherung von Ereignissen in der Administrationsserver-Datenbank beziehen, sowie Empfehlungen zur Minimierung der Anzahl der Ereignisse und der Reduzierung der Auslastung des Administrationsservers.

Standardmäßig ist in den Eigenschaften jeder Aufgabe und Richtlinie die Protokollierung aller Ereignisse aktiviert, die mit der Aufgabenausführung und der Anwendung der Richtlinie verbunden sind.

Wenn jedoch eine Aufgabe recht häufig (z. B. mehr als einmal pro Woche) auf einer recht großen Anzahl an Geräten (z. B. auf mehr als 10.000) ausgeführt wird, kann sich eine große Anzahl an Ereignissen ansammeln, welche die Datenbank überfüllen. In einem solchen Fall wird empfohlen, in den Eigenschaften der Aufgabe eine von zwei anderen Optionen festzulegen:

- **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**. In diesem Fall gehen von jedem Gerät, auf dem die Aufgabe ausgeführt wird, nur Informationen über den Start, den Verlauf und den Abschluss der Aufgabe (erfolgreich, mit Warnung oder mit einem Fehler) in die Datenbank ein.

- **Nur die Ergebnisse der Aufgabenausführung speichern**. In diesem Fall gehen von jedem Gerät, auf dem die Aufgabe ausgeführt wird, nur Informationen über den Abschluss der Aufgabe (erfolgreich, mit Warnung oder mit einem Fehler) in die Datenbank ein.

Wenn eine Richtlinie einer recht großen Anzahl an Geräten zugewiesen ist (z. B. mehr als 10.000), kann sich eine große Anzahl an Ereignissen ansammeln, welche die Datenbank überfüllen. In einem solchen Fall wird empfohlen, in den Eigenschaften der Richtlinie nur die kritischen Ereignisse auszuwählen und ihre Speicherung zu aktivieren. Es wird empfohlen, die Speicherung aller anderen Ereignisse zu deaktivieren.

Auf diese Weise reduzieren Sie die Anzahl der Ereignisse in der Datenbank, erhöhen die Ausführungsgeschwindigkeit der Szenarien, die mit der Analyse der Ereignistabelle in der Datenbank verbunden sind, und reduzieren das Risiko der Verdrängung von kritischen Ereignissen durch eine große Anzahl an Ereignissen.

Sie können außerdem die Aufbewahrungsdauer der Ereignisse reduzieren, die mit der Aufgabe (Richtlinie) verbunden sind. Standardmäßig beträgt diese Frist 7 Tage für Ereignisse, die mit einer Aufgabe verbunden sind, und 30 Tage für Ereignisse, die mit einer Richtlinie verbunden sind. Beachten Sie bei der Änderung der Aufbewahrungsfrist der Ereignisse die üblichen Arbeitsvorgänge in Ihrem Unternehmen und die Zeit, die dem Systemadministrator zur Analyse jedes Ereignisses zur Verfügung steht.

In jedem der folgenden Fälle ist es sinnvoll, die Speicherung der Ereignisse zu bearbeiten:

- Ereignisse über die Änderung von temporären Statusvarianten der Gruppenaufgaben und Ereignisse über die Anwendung von Richtlinien stellen einen wesentlichen Anteil aller Ereignisse in der Datenbank von Kaspersky Security Center dar.

- Im Kaspersky-Ereignisprotokoll erscheinen Einträge zum automatischen Löschen von Ereignissen aufgrund der Überschreitung des festgelegten Grenzwertes für die Gesamtzahl der Ereignisse, die in der Datenbank gespeichert sind.

Beachten Sie bei der Auswahl der Ereignisprotokollierungs-Optionen, dass die optimale Anzahl der Ereignisse, die von einem einzelnen Gerät stammen, maximal 20 Ereignisse pro Tag beträgt. Sie können diese Beschränkung erforderlichenfalls leicht erhöhen, jedoch nur, wenn die Anzahl an Geräten in Ihrem Netzwerk relativ klein ist (weniger als 10.000).

Besonderheiten und optimale Einstellungen bestimmter Aufgaben

Einige Aufgaben verfügen über Besonderheiten, die mit der Anzahl der Geräte im Netzwerk zusammenhängen. In diesem Abschnitt finden Sie Empfehlungen für die optimale Konfiguration solcher Aufgaben.

Die Gerätesuche, die Aufgabe zum Anlegen eines Daten-Backups, die Aufgabe zur Wartung des Administrationsservers sowie die Gruppenaufgaben zum Update von Kaspersky Endpoint Security gehören zum grundlegenden Funktionsumfang von Kaspersky Security Center.

Häufigkeit der Gerätesuche

Es wird nicht empfohlen, die voreingestellte Häufigkeit der Gerätesuche zu erhöhen, da dies zu einer übermäßigen Belastung der Domänencontroller führen kann. Es wird vielmehr empfohlen, für den Zeitplan der Abfrage eine möglichst geringe Häufigkeit festzulegen, sofern die Konfiguration Ihres Unternehmens dies erlaubt. Die nachfolgende Tabelle enthält Empfehlungen für die Berechnung des optimalen Zeitplans.

Zeitplan der Gerätesuche

Anzahl der Geräte im Netzwerk	Empfohlene Häufigkeit der Gerätesuche
Weniger als 10.000	Wie voreingestellt oder seltener
10.000 und mehr	Einmal pro Tag oder seltener

Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers und zur Wartung des Administrationsservers

Der Administrationsserver stellt während der Ausführung folgender Aufgaben seine Funktion ein:

- Backup der Daten des Administrationsservers anlegen
- Wartung des Administrationsservers

Solange diese Aufgaben ausgeführt werden, können keine Daten in die Datenbank eingehen.

Eventuell müssen Sie den Zeitplan dieser Aufgaben so anpassen, dass ihre Ausführung sich nicht mit der Ausführung anderer Aufgaben des Administrationsservers überschneidet.

Gruppenaufgaben zum Update von Kaspersky Endpoint Security

Wenn der Administrationsserver als Update-Quelle dient, wird für Gruppenaufgaben zum Update von Kaspersky Endpoint Security Version 10 und höher der Zeitplan **Nach dem Download von Updates in die Datenverwaltung** mit aktiviertem Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** empfohlen.

Wenn Sie auf jedem Verteilungspunkt eine lokale Aufgabe für den Download von Updates von den Servern von Kaspersky in den Speicher erstellt haben, wird für die Gruppenaufgabe zum Update von Kaspersky Endpoint Security ein regelmäßiger Zeitplan empfohlen. In diesem Fall muss als Zeitraum für den zufälligen Start eine Stunde angegeben werden.

Inventarisierungsaufgabe

Sie können die Auslastung der Datenbank verringern und gleichzeitig Informationen über die ausführbaren Dateien erhalten. Dazu empfehlen wir, dass Sie eine Bestandsaufnahme für Kaspersky Endpoint Security auf den Referenzgeräten durchführen, auf denen ein Standardpaket von Software installiert ist.

Die Anzahl ausführbarer Dateien, die der Administrationsserver erhält, darf 150.000 nicht überschreiten. Wenn diese Grenze erreicht wird, erhält Kaspersky Security Center keine neuen Dateien mehr.

Die Anzahl der Dateien auf einem gewöhnlichen verwalteten Client-Gerät beträgt in der Regel nicht mehr als 60.000. Die Anzahl der ausführbaren Dateien auf dem Dateiserver kann noch mehr betragen und sogar den Grenzwert von 150.000 überschreiten.

Testmessungen haben ergeben, dass auf einem Gerät unter Windows 7, auf dem nur das Programm Kaspersky Endpoint Security 11 und keine weiteren Programme installiert sind, die Ausführung der Aufgabe zur Inventarisierung folgende Ergebnisse zeigt:

- Bei deaktivierten Kontrollkästchen **Inventarisierung von DLL-Modulen** und **Inventarisierung von Script-Dateien**: ungefähr 3000 Dateien.
- Bei aktivierten Kontrollkästchen **Inventarisierung von DLL-Modulen** und **Inventarisierung von Script-Dateien**: zwischen 10.000 und 20.000 Dateien, je nach Anzahl der installierten Updates des Betriebssystems.
- Bei nur aktiviertem Kontrollkästchen **Inventarisierung von Script-Dateien**: ca. 10.000 Dateien.

Informationen zur Netzwerkauslastung zwischen dem Administrationsserver und den geschützten Geräten

Dieser Abschnitt enthält die Ergebnisse der Testmessungen des Datenverkehrs im Netzwerk unter Angabe der Bedingungen, unter denen die Messungen vorgenommen wurden. Sie können diese Informationen als Richtwerte bei der Planung der Netzwerkinfrastruktur und der Bandbreite der Kanäle innerhalb des Unternehmens (oder zwischen dem Administrationsserver und dem Unternehmen, in dem sich die geschützten Geräte befinden) verwenden. Außerdem können Sie bei Kenntnis der Bandbreite des Netzwerks ungefähr einschätzen, wie viel Zeit bestimmte Datenübertragungsoperationen in Anspruch nehmen.

Verbrauch von Datenverkehr bei der Ausführung verschiedener Szenarien

Die nachfolgende Tabelle enthält die Ergebnisse der Testmessungen des Datenverkehrs zwischen dem Administrationsserver und dem verwalteten Gerät während der Ausführung verschiedener Szenarien.

Die Synchronisierung des Geräts mit dem Administrationsserver erfolgt standardmäßig einmal alle 15 Minuten oder seltener. Wenn Sie jedoch die Einstellungen einer Richtlinie oder einer Aufgabe auf dem Administrationsserver ändern, wird eine vorzeitige Synchronisierung der Geräte vorgenommen, auf die diese Richtlinie (Aufgabe) angewendet wird, und die neuen Einstellungen werden an die Geräte übermittelt.

Datenverkehr zwischen dem Administrationsserver und dem verwalteten Gerät

Szenario	Datenverkehr vom Administrationsserver zu jedem verwalteten Gerät	Datenverkehr von jedem verwalteten Gerät zum Administrationsserver
Installation von Kaspersky Endpoint Security 11.7 für Windows mit den aktualisierten Datenbanken	390 MB	3,3 MB
Installation des Administrationsagenten	75 MB	397 KB
Gemeinsame Installation des Administrationsagenten und Kaspersky Endpoint Security 11.7 für Windows	459 MB	3.6 MB
Erstmaliges Update der Antiviren-Datenbanken ohne Update der Datenbanken im Paket (bei Ablehnung der Teilnahme an Kaspersky Security Network)	113 MB	1,8 MB
Tägliches Update der Antiviren-Datenbanken (bei aktivierter Teilnahme an Kaspersky Security Network)	22 MB	373 MB
Erstmalige Synchronisierung vor dem Datenbanken-Update auf dem Gerät (Übermittlung von Richtlinien und Aufgaben)	382 KB	446 KB

Szenario	Datenverkehr vom Administrationsserver zu jedem verwalteten Gerät	Datenverkehr von jedem verwalteten Gerät zum Administrationsserver
Erstmalige Synchronisierung nach dem Datenbanken-Update auf dem Gerät	20 KB	157 KB
Synchronisierung bei fehlenden Änderungen auf dem Administrationsserver (nach Zeitplan)	18 KB	23 KB
Synchronisierung bei Änderung einer Einstellung in der Gruppenrichtlinie (vorzeitig, sofort nach der Änderung)	19 KB	20 KB
Synchronisierung bei Änderung einer Einstellung in der Gruppenaufgabe (vorzeitig, sofort nach der Änderung)	14 KB	11 KB
Erzwungene Synchronisierung	110 KB	109 KB
Ereignis **Virus gefunden** (1 Virus)	44 KB	50 KB
Ereignis **Virus gefunden** (10 Viren)	58 KB	77 KB
Einmaliger Datenverkehr nach Aktivierung der Programm-Registry-Liste	bis zu 10 KB	bis zu 12 KB
Täglicher Datenverkehr, wenn die Programm-Registry-Liste aktiviert ist	bis zu 840 KB	bis zu 1 MB

Mittleren Verbrauch von Datenverkehr in 24 Stunden

Die durchschnittliche Nutzung des Datenverkehrs stellt sich zwischen dem Administrationsserver und einem verwalteten Gerät innerhalb von 24-Stunden wie folgt dar:

- Der Datenverkehr vom Administrationsserver zum verwalteten Gerät beträgt 840 KB.
- Der Datenverkehr vom verwalteten Gerät zum Administrationsserver beträgt 1 MB.

Der Datenverkehr wurde unter folgenden Bedingungen gemessen:

- Auf dem verwalteten Gerät waren Administrationsagent und Kaspersky Endpoint Security 11.6 für Windows installiert.
- Dem Gerät wurde kein Verteilungspunkt zugewiesen.
- Das Schwachstellen- und Patch-Management war nicht aktiviert.
- Das Synchronisierungsintervall mit dem Administrationsserver betrug 15 Minuten.

Anfrage an den Technischen Support

Dieser Abschnitt beschreibt, wie und unter welchen Bedingungen Sie technischen Support erhalten.

Wie Sie technischen Support erhalten können

Wenn Sie weder in der Dokumentation von Kaspersky Security Center noch in den anderen Informationsquellen zu Kaspersky Security Center keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky. Die Mitarbeiter des Technischen Supports beantworten alle Fragen zur Installation und Verwendung von Kaspersky Security Center.

> Kaspersky bietet die Unterstützung für Kaspersky Security Center im Rahmen dessen Lebenszyklus' an (siehe Support-Webseite mit dem Lebenszyklus der Anwendung). Bitte beachten Sie die Support-Richtlinien, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit dem Technischen Support ist auf folgende Weise möglich:

- Durch das Aufrufen der Website des Technischen Supports
- Durch das Senden einer Anfrage an den Technischen Support über das Portal Kaspersky CompanyAccount

Technischer Support mit Kaspersky CompanyAccount

Kaspersky CompanyAccount ist ein Portal für Unternehmen, die Kaspersky-Programme verwenden. Das Portal Kaspersky CompanyAccount dient der Interaktion zwischen Benutzern und Kaspersky-Experten mithilfe von Online-Anfragen. Mithilfe von Kaspersky CompanyAccount können Sie den Status Ihrer Online-Anfragen verfolgen und eine Chronik mit allen Anfragen speichern.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Kontos können Sie die Online-Anfragen der bei Kaspersky registrierten Mitarbeiter zentral verwalten und die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in den folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch

- Russisch
- Französisch
- Japanisch

Weitere Informationen über Kaspersky CompanyAccount finden Sie auf der Webseite des Technischen Supports.

Dump-Dateien des Administrationsservers abrufen

Die Dump-Dateien des Administrationsservers enthalten alle Informationen über die Prozesse des Administrationsservers zu einem bestimmten Zeitpunkt. Die Dump-Dateien des Administrationsservers werden im Ordner "%ALLUSERSPROFILE%\Programmdaten\KasperskyLab\adminkit\~dumps" gespeichert. Die Dump-Dateien werden so lange gespeichert, wie sich Kaspersky Security Center in Verwendung befindet. Wenn Kaspersky Security Center entfernt wird, werden auch die Dump-Dateien endgültig gelöscht. Dump-Dateien werden nicht automatisch an Kaspersky übertragen.

Wenn der Administrationsserver abstürzt, können Sie sich an den Technischen Support von Kaspersky wenden. Ein Spezialist des Technischen Supports kann Sie bitten, die Dump-Dateien des Administrationsservers zur weiteren Analyse an Kaspersky zu senden.

Dump-Dateien können personenbezogene Daten enthalten. Es wird empfohlen, die Informationen vor dem Senden an Kaspersky vor unbefugtem Zugriff zu schützen.

Informationsquellen über das Programm

Seite von Kaspersky Security Center auf der Website von Kaspersky

Auf der Kaspersky-Website im Abschnitt zu Kaspersky Security Center finden Sie allgemeine Informationen über die Anwendung, ihre Funktionen und Besonderheiten.

Seite von Kaspersky Security Center in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt der Website des Technischen Supports von Kaspersky.

Auf der Seite von Kaspersky Security Center in der Wissensdatenbank finden Sie Artikel mit nützlichen Informationen, Tipps und Antworten auf häufige Fragen zu Erwerb, Installation und Nutzung des Programms.

Neben Fragen zu Kaspersky Security Center können die Artikel auch andere Kaspersky-Anwendungen betreffen. Artikel in der Wissensdatenbank können auch Neuigkeiten über den Technischen Support enthalten.

In der Community über Kaspersky-Anwendungen diskutieren

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie diese mit den Experten von Kaspersky und mit anderen Benutzern in unserem Forum diskutieren.

Im Forum können Sie Diskussionsthemen nachlesen, Kommentare schreiben und neue Diskussionsthemen erstellen.

> Um auf die Website-Ressourcen zuzugreifen, ist eine Internetverbindung erforderlich.

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support.

Glossar

Administrationsagent

Eine Komponente von Kaspersky Security Center, mit deren Hilfe die Interaktion zwischen dem Administrationsserver und den Kaspersky-Anwendungen ermöglicht wird, die auf einem bestimmten Netzwerk-Knoten (Workstation oder Server) installiert sind. Diese Komponente ist für alle von dem Unternehmen entwickelten Anwendung für Microsoft® Windows® einheitlich. Für Kaspersky-Anwendungen, die für Unix-artige Betriebssysteme und macOS entwickelt wurden, gibt es separate Versionen des Administrationsagenten.

Administrationsgruppe

Ein Satz von Geräten, die nach Funktion und installierten Kaspersky-Anwendungen gruppiert sind. Geräte sind zur erleichterten Verwaltung als einzelne Entität gruppiert. Eine Gruppe kann andere Gruppen beinhalten. Für jede installierte Anwendung in der Gruppe können Gruppenrichtlinien und Gruppenaufgaben erstellt werden.

Administrationsserver

Eine Komponente von Kaspersky Security Center, die Informationen über alle Kaspersky-Anwendungen, die innerhalb des Unternehmensnetzwerks installiert sind, zentral speichert. Sie kann auch zur Verwaltung dieser Anwendungen verwendet werden.

Administrationsserver-Client (Client-Gerät)

Gerät, Server oder Workstation, auf welchem bzw. welcher der Administrationsagent installiert ist und verwaltete Kaspersky-Anwendungen ausgeführt werden.

Administrator des Anbieters

Mitarbeiter eines Anbieters von Antiviren-Schutz. Dieser Administrator führt Installations- und Verwaltungsaufträge für Antiviren-Schutzsysteme auf der Grundlage von Antiviren-Produkten von Kaspersky durch und bietet darüber hinaus technischen Support für Kunden.

Administrator von Kaspersky Security Center

Person, die über das zentralisierte Remote-Verwaltungssystem Kaspersky Security Center die die Anwendungsvorgänge verwaltet.

Administrator-Arbeitsplatz

Ein Gerät, auf dem die Verwaltungskonsole installiert ist, oder das Sie zum Öffnen der Kaspersky Security Center Web Console verwenden. Diese Komponente stellt eine Verwaltungsschnittstelle von Kaspersky Security Center bereit.

Der Administrator-Arbeitsplatz wird zur Konfiguration und Verwaltung der Serverseite von Kaspersky Security Center verwendet. Mithilfe des Administrator-Arbeitsplatzes erstellt und verwaltet der Administrator ein zentralisierten Antiviren-Schutzsystem für ein Unternehmens-LAN auf der Grundlage von Kaspersky-Anwendungen.

Administratorberechtigungen

Stufe der Benutzerberechtigungen und Rechte, die für die Verwaltung von Exchange-Objekten innerhalb einer Exchange-Organisation erforderlich sind.

Aktiver Schlüssel

Ein Schlüssel, der momentan von der Anwendung verwendet wird.

Amazon EC2-Instance

Virtuelle Maschine, die auf der Grundlage eines AMI-Abbilds mithilfe von Amazon Web Services erstellt wurde.

Amazon Machine Image (AMI)

Vorlage, in der die Softwarekonfiguration enthalten ist, die für die Ausführung der virtuellen Maschine erforderlich ist. Mehrere Instances können auf der Grundlage eines einzelnen AMI erstellt werden.

Anbieter von Antiviren-Schutz

Ein Unternehmen, das für ein Kundenunternehmen einen Antiviren-Schutz auf der Grundlage von Lösungen von Kaspersky bereitstellt.

Antiviren-Datenbanken

Datenbanken, die Informationen über diejenigen Bedrohungen der Computersicherheit enthalten, die Kaspersky zum Zeitpunkt des Erscheinens der Antiviren-Datenbanken bekannt sind. Durch die Eintragungen in den Antiviren-Datenbanken kann in den untersuchten Objekten schädlicher Code erkannt werden. Antiviren-Datenbanken werden von den Experten von Kaspersky erstellt und stündlich aktualisiert.

App Store

Komponente von Kaspersky Security Center. Der App Store wird zur Installation von Apps auf Android-Geräten von Benutzern verwendet. Der App Store erlaubt Ihnen, die APK-Dateien von Apps und Links zu Apps in Google Play zu veröffentlichen.

Aufgabe

Funktionen, die eine Kaspersky-Anwendung ausführt, werden als Aufgaben implementiert, beispielsweise: Echtzeitschutz von Dateien, Vollständige Untersuchung des Computers und Datenbanken-Update.

Aufgabe für eine Reihe von Geräten

Aufgabe, die einer Auswahl von Client-Geräten aus beliebigen Administrationsgruppen zugewiesen ist und auf diesen Geräten ausgeführt wird.

Aufgabeneinstellungen

Programmeinstellungen, die spezifisch für die einzelnen Aufgabentypen sind.

Authentifizierungsagent

Schnittstellen, mit der Sie die Authentifizierung für den Zugriff auf verschlüsselte Festplatten abschließen und das Betriebssystem nach der Verschlüsselung der startbaren Festplatte laden können.

AWS Application Program Interface (AWS API)

Anwendungsprogrammierschnittstelle der AWS-Plattform, die von Kaspersky Security Center verwendet wird. Insbesondere werden AWS API-Instrumente zur Abfrage von Cloud-Segmenten und Installation des Administrationsagenten auf Instances verwendet.

AWS IAM-Zugriffsschlüssel

Kombination, die aus der Schlüssel-ID (etwa wie "AKIAIOSFODNN7EXAMPLE") und dem geheimen Schlüssel (etwa wie "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY") besteht. Dieses Paar gehört zum IAM-Benutzer und wird verwendet, um Zugriff auf AWS-Dienste zu erhalten.

AWS-Managementkonsole

Weboberfläche zum Anzeigen und Verwalten von AWS-Ressourcen. Die AWS-Managementkonsole ist im Internet unter https://aws.amazon.com/de/console/ verfügbar.

Backup-Ordner

Spezieller Ordner zum Speichern von Kopien der Daten des Administrationsservers, die mithilfe des Backup-Tools erstellt werden.

Broadcast-Domäne

Logischer Bereich eines Netzwerks, in dem alle Knoten mithilfe eines Broadcast-Kanals auf OSI-Ebene (Open Systems Interconnection Basic Reference Model) Daten austauschen können.

Client-Administrator

Mitarbeiter eines Kundenunternehmens, der für die Überwachung des Antiviren-Schutzstatus verantwortlich ist.

Cloud Discovery

Cloud Discovery ist eine Komponente des Cloud Access Security Brokers (CASB), der die Cloud-Infrastruktur eines Unternehmens schützt. Cloud Discovery verwaltet den Benutzerzugriff auf Cloud-Dienste. Solche Cloud-Dienste sind beispielsweise Microsoft Teams, Salesforce und Microsoft Office 365. Die Cloud-Dienste werden in Kategorien wie *Datenaustausch*, *Messenger* oder *E-Mail* eingeteilt.

Cloud-Umgebung

Virtuelle Maschinen und andere virtuelle Ressourcen, die auf einer Cloud-Plattform basieren und in Netzwerken kombiniert sind.

Daten-Backup des Administrationsservers

Kopieren der Daten des Administrationsservers als Backup und zur anschließenden Wiederherstellung mithilfe des Backup-Tools. Das Tool kann Folgendes speichern:

- Administrationsserver-Datenbank (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse)
- Konfigurationsdaten über die Struktur von Administrationsgruppen und Client-Geräten

- Datenverwaltung der Installationsdateien zur Remote-Installation von Anwendungen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Demilitarisierte Zone (DMZ)

Die demilitarisierte Zone ist ein Segment eines lokalen Netzwerks, das Server enthält, die auf Anfragen aus dem globalen Internet antworten. Um die Sicherheit des lokalen Netzwerks einer Organisation zu gewährleisten, wird der Zugriff auf das LAN aus der demilitarisierten Zone mithilfe einer Firewall geschützt.

Direkte Anwendungsverwaltung

Anwendungsverwaltung über eine lokale Schnittstelle.

Ereignis-Datenverwaltung

Ein Teil der Administrationsserver-Datenbank, der Speicherung von Informationen über Ereignisse im Kaspersky Security Center dient.

Ereigniskategorie des Patches

Attribut des Patches. Es gibt fünf Ereigniskategorien für Microsoft-Patches und Drittanbieter-Patches:

- Kritisch
- Hoch
- Normal
- Niedrig
- Unbekannt

Die Ereigniskategorie eines Drittanbieter-Patches oder Microsoft-Patches wird durch die ungünstigste Signifikanz unter den Schwachstellen bestimmt, die der Patch beheben soll.

Erzwungene Installation

Methode zur Remote-Installation von Kaspersky-Anwendungen, die Ihnen erlaubt, Software auf bestimmten Client-Geräten zu installieren. Für eine erfolgreiche erzwungene Installation muss das für die Aufgabe verwendete Konto über ausreichende Berechtigungen zum Remote-Start von Programmen auf Client-Geräten verfügen. Diese Methode wird für die Installation von Programmen auf Geräten empfohlen, die unter Microsoft Windows-Betriebssystemen laufen und diese Funktion unterstützen.

Gerät mit Schutz auf UEFI-Ebene

Gerät mit einer für UEFI vorgesehenen Lösung oder Anwendung von Kaspersky, die auf BIOS-Ebene integriert wurde. Der integrierte Schutz gewährleistet die Sicherheit des Geräts bereits ab Beginn des Systemstarts, während der Schutz für Geräte, die keine integrierte Software haben, erst nach dem Start der Sicherheitsanwendung in Aktion tritt.

Gerätebesitzer

Der Gerätebesitzer ist ein Benutzer, an den sich der Administrator wenden kann, wenn Bedarf zur Durchführung bestimmter Operationen auf einem Gerät besteht.

Geteiltes Zertifikat

Ein Zertifikat, das zur Identifizierung des mobilen Geräts des Benutzers dient.

Grenzwert für Virenaktivität

Maximal zugelassene Anzahl der Ereignisse des festgelegten Typs innerhalb eine beschränkten Zeit: Wird diese Zahl überschritten, wird das als erhöhte Virenaktivität und Bedrohung eines Virenangriffs betrachtet. Diese Funktion ist während der Dauer von Virenangriff von Bedeutung, da sie Administratoren ermöglicht, rechtzeitig auf Bedrohungen durch Virenangriffen zu reagieren.

Gruppenaufgabe

Aufgabe, die für eine Administrationsgruppe definiert und auf allen Client-Geräten innerhalb dieser Administrationsgruppe ausgeführt wird.

Gültigkeitsdauer der Lizenz

Zeitraum, in dem Ihnen die Funktionen der Anwendung zur Verfügung stehen und Sie berechtigt sind, zusätzliche Leistungen in Anspruch zu nehmen. Die Ihnen zur Verfügung stehenden Leistungen hängen vom Lizenztyp ab.

Härtungsleitfaden

Eine Sammlung an Empfehlungen und Funktionen zur Konfiguration von Kaspersky Security Center und seinen Komponenten, mit dem Ziel, das Risiko einer Kompromittierung zu verringern.

Home-Administrationsserver

Der Home-Administrationsserver ist der Administrationsserver, der während der Installation des Administrationsagenten festgelegt wurde. Der Home-Administrationsserver kann in Einstellungen der Verbindungsprofile des Administrationsagenten verwendet werden.

HTTPS

Sicheres Protokoll zur Datenübertragung mittels Verschlüsselung zwischen einem Browser und einem Webserver. Um Zugriff auf beschränkte Informationen, wie etwa Unternehmensdaten oder Finanzdaten, zu erhalten, wird HTTPS verwendet.

IAM-Benutzer

Benutzer von AWS-Diensten. Ein IAM-Benutzer kann die Berechtigungen zur Durchführung von Abfrage von Cloud-Segmenten haben.

IAM-Rolle

Satz von Berechtigungen zur Durchführung von Anfragen in AWS-basierten Diensten. IAM-Rollen sind nicht mit einem spezifischen Benutzer oder einer bestimmten Gruppe verknüpft, sie stellen Zugriffsrechte ohne AWS IAM-Zugriffsschlüssel bereit. Sie können eine IAM-Rolle IAM-Benutzern, EC2-Instances und AWS-basierten Programmen oder Diensten zuweisen.

Identitäts- und Zugriffsverwaltung (IAM)

AWS-Dienst, der eine Verwaltung des Benutzerzugriffs auf andere AWS-Dienste und Ressourcen ermöglicht.

Inkompatibles Programm

Antiviren-Anwendung eines fremden Entwicklers oder Kaspersky-Anwendung, welche die Verwaltung über Kaspersky Security Center nicht unterstützt.

Installationspaket

Zusammenstellung von Dateien, die für die Remote-Installation einer Kaspersky-Anwendung mithilfe des Remote-Verwaltungssystems von Kaspersky Security Center erstellt wurde. Das Installationspaket enthält eine Reihe von Einstellungen, die für die Installation und Inbetriebnahme der Anwendung nach der Installation benötigt werden. Die Einstellungen entsprechen der Standardkonfiguration der Anwendung. Das Installationspaket wird mithilfe von Dateien mit der Erweiterung .kpd und .kud erstellt, die im Lieferumfang der Anwendung enthalten sind.

Interne Benutzer

Die Benutzerkonten der internen Benutzer werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Innerhalb der Funktionen von Kaspersky Security Center verfügen die internen Benutzer über die Berechtigungen tatsächlicher Benutzer.

Benutzerkonten der internen Benutzer werden nur innerhalb von Kaspersky Security Center erstellt und verwendet. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center.

iOS MDM-Gerät

Mobiles Gerät, das über das iOS MDM-Protokoll mit dem iOS MDM-Server verbunden ist. Geräte mit dem Betriebssystem iOS können mithilfe des iOS MDM-Protokolls verbunden und verwaltet werden.

iOS MDM-Profil

Zusammenstellung von Einstellungen zur Verbindung von mobilen iOS-Geräten mit dem Administrationsserver. Der Benutzer installiert ein iOS MDM-Profil auf einem mobilen Gerät, worauf sich das mobile Gerät mit dem Administrationsserver verbindet.

iOS MDM-Server

Komponente von Kaspersky Security Center, die auf einem Client-Gerät installiert ist, die eine Verbindung von mobilen iOS-Geräten mit dem Administrationsserver und die Verwaltung von mobilen iOS-Geräten über Apple Push Notifications (APNs) ermöglicht.

JavaScript

Programmiersprache, mit der die Leistungsfähigkeit von Webseiten erweitert wird. Webseiten, die mithilfe von JavaScript erstellt wurden, können Funktionen (beispielsweise die Ansicht von Schnittstellenelementen ändern oder zusätzliche Fenster öffnen) ausführen, ohne die Webseite mit neuen Daten aus einem Webserver zu aktualisieren. Um Seiten anzuzeigen, die mithilfe von JavaScript erstellt wurden, aktivieren Sie die Unterstützung von JavaScript in der Konfiguration Ihres Browsers.

Kaspersky Private Security Network (KPSN)

Die Lösung Kaspersky Private Security Network gewährt Benutzern von Geräten, auf denen Kaspersky-Anwendungen installiert sind, Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network sowie auf andere statistische Daten, ohne dass Daten von ihren Geräten an Kaspersky Security Network gesendet werden müssen. Kaspersky Private Security Network richtet sich an Unternehmenskunden, die aus einem der folgenden Gründe nicht an Kaspersky Security Network teilnehmen können:

- Die Geräte haben keine Internetverbindung.

- Die Übermittlung von Daten an einen Punkt außerhalb des Landes oder des lokalen Unternehmensnetzwerks ist gesetzlich oder aufgrund von Sicherheitsrichtlinien des Unternehmens untersagt.

Kaspersky Security Center Operator

Benutzer, der den Status und Betrieb eines Schutzsystems überwacht, das mithilfe von Kaspersky Security Center verwaltet wird.

Kaspersky Security Center System Health Validator (SHV)

Komponente von Kaspersky Security Center, die zur Überprüfung der Einsatzfähigkeit des Betriebssystems im Fall von gleichzeitigem Betrieb von Kaspersky Security Center und Microsoft NAP dient.

Kaspersky Security Center Webserver

Komponente von Kaspersky Security Center, die gemeinsam mit dem Administrationsserver installiert wird. Der Webserver dient dazu, autonome Installationspakete, iOS MDM-Profile sowie Dateien aus einem freigegebenen Ordner im Netzwerk zu übertragen.

Kaspersky Security Network (KSN)

Eine Infrastruktur aus Cloud-Diensten, die Zugriff auf die Kaspersky-Datenbank bietet. Diese Datenbank enthält laufend aktualisierte Informationen über die Reputation von Dateien, Webressourcen und Software. Kaspersky Security Network gewährleistet eine schnellere Reaktion der Kaspersky-Anwendungen auf Bedrohungen, erhöht die Leistungsfähigkeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

Kaspersky-Update-Server

HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen.

KES-Gerät

Mobiles Gerät, das mit dem Kaspersky Security Center Administrationsserver verbunden ist und mittels Kaspersky Endpoint Security für Android per App verwaltet wird.

Konfigurationsprofil

Richtlinie, die eine Zusammenstellung von Einstellungen und Einschränkungen für ein mobiles iOS MDM-Gerät enthält.

Lightweight Nagent (LWNGT)

Ein Protokoll für die Interaktion mit Kaspersky Endpoint Security auf Mobilgeräten. LWNGT (auch mobiles Protokoll genannt) fungiert als Administrationsagent, ohne dass der Administrationsagent tatsächlich auf Mobilgeräten installiert sein muss.

Lizenzierte Anwendungsgruppe

Gruppe von Anwendungen, die auf der Grundlage von Kriterien erstellt wird, die vom Administrator festgelegt werden (beispielsweise nach Hersteller), für die Statistiken zu den Installationen auf Client-Geräten geführt werden.

Lokale Aufgabe

Aufgabe, die auf einem einzelnen Client-Computer definiert wurde und ausgeführt wird.

Lokale Installation

Installation einer Sicherheitsanwendung auf einem Gerät in einem Unternehmensnetzwerk, die entweder den manuellen Start der Installation über das Programmpaket der Sicherheitsanwendung oder den manuellen Start eines veröffentlichten Installationspakets, das zuvor auf das Gerät heruntergeladen wurde, voraussetzt.

Manuelle Installation

Installation einer Sicherheitsanwendung aus dem Programmpaket auf einem Gerät im Unternehmensnetzwerk. Manuelle Installation erfordert die Einbeziehung eines Administrators oder anderen IT-Spezialisten. Im Normalfall wird eine manuelle Installation durchgeführt, wenn die Remote-Installation mit einem Fehler beendet wurde.

MITM-Angriff

Man In The Middle Dies beschreibt einen Angriff auf die IT-Infrastruktur eines Unternehmens, bei dem ein Hacker die Kommunikationsverbindung zwischen zwei Zugriffspunkten übernimmt, weiterleitet und gegebenenfalls die Verbindung zwischen diesen Zugriffspunkten verändert.

Network Location Awareness (NLA)

Ein Windows-Dienst, der einem Betriebssystem hilft, das aktuelle Netzwerk zu identifizieren. NLA erkennt Änderungen des Netzwerks und passt die Sicherheitskonfiguration des Geräts an.

Netzwerk-Antiviren-Schutz

Satz von technischen und organisatorischen Maßnahmen, die das Risiko senken, dass Viren und Spam in das Netzwerk einer Organisation eindringen, und die Netzwerkangriffe, Phishing und andere Bedrohungen verhindern. Die Sicherheit des Netzwerks steigt, wenn Sie Sicherheitsanwendungen und Dienste nutzen, und wenn Sie die Sicherheitsrichtlinie des Unternehmens übernehmen und einhalten.

Netzwerk-Schutzstatus

Aktueller Schutzstatus, der die Sicherheit der Geräte im Unternehmensnetzwerk definiert. Der Status des Netzwerk-Schutzstatus beinhaltet Faktoren wie installierte Sicherheitsanwendungen, Verwendung von Lizenzschlüsseln sowie Anzahl und Typen der gefundenen Bedrohungen.

Programmeinstellungen

Anwendungseinstellungen, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb der Anwendung regeln, zum Beispiel Leistungseinstellungen, Berichtseinstellungen und Backup-Einstellungen.

Provisioning-Profil

Zusammenstellung von Einstellungen für die Ausführung von Anwendungen auf mobilen iOS-Geräten. Ein Provisioning-Profil enthält Informationen zur Lizenz und ist mit einer bestimmten Anwendung verbunden.

Remote-Installation

Installation von Kaspersky-Anwendungen mithilfe der von Kaspersky Security Center bereitgestellten Dienste.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen einer Anwendung und verwaltet die Möglichkeit, diese Anwendung auf Computern innerhalb einer Administrationsgruppe zu konfigurieren. Für jede Anwendung muss eine eigene Richtlinie erstellt werden. Sie können mehrere Richtlinien für Anwendungen, die auf Computern in mehreren Administrationsgruppen installiert sind, erstellen, es kann jedoch innerhalb einer Administrationsgruppe immer nur eine Richtlinie auf eine Anwendung angewendet werden.

Schlüsseldatei

Datei im Format xxxxxxxx.key, die ermöglicht, eine Kaspersky-Anwendung unter eine Test- oder kommerziellen Lizenz zu nutzen.

Schutzstatus

Aktueller Schutzstatus, der die Stufe der Computersicherheit widerspiegelt.

Schwachstelle

Ein Fehler in einem Betriebssystem oder einem Programm, der von Entwicklern von Schadsoftware benutzt werden kann, um in das Betriebssystem oder Programm einzudringen und dessen Integrität zu gefährden. Das Vorliegen einer großen Anzahl von Schwachstellen in einem Betriebssystem macht dieses unzuverlässig, da Viren, die in das Betriebssystem eingedrungen sind, zu Ausführungsfehlern im System selbst sowie in den installierten Programmen führen können.

Server für mobile Geräte

Komponente von Kaspersky Security Center, die den Zugriff auf mobile Geräte bereitstellt und Ihnen erlaubt, diese über die Verwaltungskonsole zu verwalten.

Signifikanz des Ereignisses

Eigenschaft eines Ereignisses, das während des Betriebs einer Kaspersky-Anwendung aufgetreten ist. Es gibt folgende Varianten für die Signifikanz:

- Kritisches Ereignis
- Funktionsfehler
- Warnung
- Information

Ereignisse desselben Typs können abhängig von der Situation, in der das Ereignis aufgetreten ist, unterschiedliche Signifikanzen aufweisen.

SSL

Datenverschlüsselungsprotokoll, das im Internet und in lokalen Netzwerken verwendet wird. Das SSL-Protokoll (Secure Sockets Layer) wird in Web-Anwendungen verwendet, um eine sichere Verbindung zwischen einem Client und einem Server herzustellen.

Update

Das Verfahren zum Ersetzen oder Hinzufügen von neuen Dateien (Datenbanken oder Anwendungsmodule), die von den Kaspersky-Update-Servern abgerufen werden.

Upgraden von Kaspersky Security Center (Aktualisieren)

Das Verfahren zur Installation einer neueren Version von Kaspersky Security Center auf einem Gerät, auf dem eine ältere Version dieser Anwendung installiert ist.

Verbindungs-Gateway

Ein *Verbindungs-Gateway* ist ein Administrationsagent, der in einem speziellen Modus ausgeführt wird. Ein Verbindungs-Gateway akzeptiert Verbindungen von anderen Administrationsagenten und tunnelt diese zum Administrationsserver mittels einer eigenen Verbindung zum Server. Anstatt wie gewöhnliche Administrationsagenten selbst eine Verbindung zum Administrationsserver herzustellen, wartet ein Verbindungs-Gateway auf eine Verbindung vom Administrationsserver.

Verfügbares Update

Eine Zusammenstellung von Updates für Module der Kaspersky-Anwendungen einschließlich kritischer Updates, die sich über einen bestimmten Zeitraum angesammelt haben, und Änderungen an der Programmarchitektur.

Verteilungspunkt

Computer, auf dem der Administrationsagent installiert ist und der zur Update-Verteilung, zur Remote-Installation von Anwendungen und zum Empfangen von Informationen über Computer in einer Administrationsgruppe und/oder Broadcasting-Domäne verwendet wird. Verteilungspunkte dienen dazu, die Belastung auf dem Administrationsserver während der Update-Verteilung zu verringern und den Netzwerkdatenverkehr zu optimieren. Verteilungspunkte können automatisch vom Administrationsserver oder manuell vom Administrator zugewiesen werden. Der Verteilungspunkt war in früheren Versionen als Update-Agent bekannt.

Verwaltete Geräte

Geräte in Unternehmensnetzwerken, die in einer Administrationsgruppe enthalten sind.

Verwaltungs-Plug-in

Spezielle Komponente, welche die Schnittstelle für die Programmverwaltung durch die Verwaltungskonsole bereitstellt. Jedes Programm verfügt über sein eigens Plug-in. Es ist in allen Kaspersky-Anwendungen enthalten und kann mithilfe von Kaspersky Security Center verwaltet werden.

Verwaltungskonsole

Eine Komponente des Windows-basierten Kaspersky Security Center (auch "MMC-basierte Verwaltungskonsole" genannt). Diese Komponente stellt eine Benutzeroberfläche für die administrativen Dienste des Administrationsservers und des Administrationsagenten bereit.

Virenangriff

Eine Serie von vorsätzlichen Versuchen, ein Gerät mit einem Virus zu infizieren.

Virtueller Administrationsserver

Komponente von Kaspersky Security Center, die zur Verwaltung des Schutzsystems für das Netzwerk eines Kundenunternehmens dient.

Ein virtueller Administrationsserver stellt einen besonderen Fall eines sekundären Administrationsservers dar und weist im Vergleich zu einem physikalischen Administrationsserver folgende Einschränkungen auf:

- Ein virtueller Administrationsserver kann nur auf einem primären Administrationsserver erstellt werden.
- Ein virtueller Administrationsserver verwendet während seines Betriebs die Datenbank des primären Administrationsservers. Aufgaben zum Anlegen eines Daten-Backups und zur Wiederherstellung von Dateien, sowie Aufgaben zur Suche nach Updates und Downloadaufgaben werden von einem virtuellen Administrationsserver nicht unterstützt.
- Für virtuelle Server können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).

Wiederherstellung

Wiederherstellung des ursprünglichen Objekts aus der Quarantäne oder dem Backup in seinem ursprünglichen Ordner, wo das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einem benutzerdefinierten Ordner.

Wiederherstellung der Daten des Administrationsservers

Wiederherstellung der Daten des Administrationsservers aus den Informationen, die mithilfe des Backup-Tools im Backup gespeichert wurden. Das Tool kann Folgendes wiederherstellen:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse)
- Konfigurationsdaten über die Struktur von Administrationsgruppen und Client-Geräten
- Datenverwaltung der Installationsdateien zur Remote-Installation von Anwendungen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Windows Server Update-Dienst (WSUS)

Programm, das zur Verteilung von Updates für Microsoft-Programme auf Computern der Benutzer im Netzwerk eines Unternehmens verwendet wird.

Zentralisierte Anwendungsverwaltung

Remote-Anwendungsverwaltung mithilfe der Verwaltungsdienste, die in Kaspersky Security Center bereitgestellt werden.

Zertifikat des Administrationsservers

Das Zertifikat, das der Administrationsserver für folgende Zwecke verwendet:

- Authentifizierung des Administrationsservers bei der Verbindung mit der MMC-basierten Verwaltungskonsole oder der Kaspersky Security Center Web Console
- Sichere Interaktion zwischen dem Administrationsserver und den Administrationsagenten auf verwalteten Geräten
- Authentifizierung von Administrationsservern beim Verbinden eines primären Administrationsservers mit einem sekundären Administrationsserver

Das Zertifikat wird bei der Installation des Administrationsservers automatisch erstellt und auf dem Administrationsserver gespeichert.

Zusätzlicher Lizenzschlüssel (oder Reserve-Lizenzschlüssel)

Ein Schlüssel, der das Recht auf Nutzung der Anwendung bestätigt, jedoch im Augenblick nicht aktiviert ist.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittanbietern finden Sie in der Datei legal_notices.txt, die sich im Installationsverzeichnis des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash, Shockwave und PostScript sind in den USA und/oder anderen Ländern eingetragene Markenzeichen oder Markenzeichen von Adobe.

AMD, AMD64 sind Warenzeichen oder eingetragene Marken von Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2 und AWS Marketplace sind Markenzeichen von Amazon.com, Inc. oder von verbundenen Unternehmen.

Apache ist entweder ein eingetragenes Markenzeichen oder ein Markenzeichen der Apache Software Foundation in den USA und anderen Ländern.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime und Touch ID sind Markenzeichen von Apple Inc.

Arm ist ein eingetragenes Markenzeichen von Arm Limited (oder seinen Tochtergesellschaften) in den USA und/oder anderswo.

Die Bluetooth-Wortmarke und die Bluetooth-Logos sind Eigentum der Bluetooth SIG, Inc.

Ubuntu und LTS sind eingetragene Markenzeichen von Canonical Ltd.

Cisco Systems, Cisco, Cisco Jabber und IOS sind eingetragene Markenzeichen von Cisco Systems, Inc. und/oder ihren Tochtergesellschaften in den USA und in anderen Ländern.

Citrix und XenServer sind entweder eingetragene Markenzeichen oder Markenzeichen der Cloud Software Group, Inc. und/oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

Corel ist eine Marke oder eingetragene Marke der Corel Corporation und/oder ihrer Tochtergesellschaften in Kanada, den USA und/oder anderen Ländern.

Cloudflare, das Cloudflare-Logo und Cloudflare Workers sind Markenzeichen und/oder eingetragene Markenzeichen von Cloudflare, Inc. in den Vereinigten Staaten und anderen Gerichtsbarkeiten.

Dropbox ist ein Markenzeichen von Dropbox, Inc.

Radmin ist ein eingetragenes Markenzeichen von Famatech.

Firebird ist ein eingetragenes Markenzeichen der Firebird-Stiftung.

Foxit ist ein eingetragenes Markenzeichen der Foxit Corporation.

Das Logo FreeBSD ist ein eingetragenes Warenzeichen der Stiftung The FreeBSD.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS und YouTube sind Markenzeichen von Google LLC.

EulerOS, FusionCompute und FusionSphere sind Markenzeichen von Huawei Technologies Co., Ltd.

Intel, Core und Xeon sind Markenzeichen der Intel Corporation oder ihrer Tochtergesellschaften.

IBM und QRadar sind Markenzeichen der International Business Machines Corporation und in vielen Ländern der Welt eingetragen.

Node.js ist ein Markenzeichen von Joyent, Inc.

Linux ist das eingetragene Markenzeichen von Linus Torvalds in den USA und anderen Ländern.

Logitech ist entweder ein Markenzeichen oder ein eingetragenes Markenzeichen von Logitech in den USA und anderen Ländern.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista und Windows Azure sind Markenzeichen der Microsoft-Unternehmensgruppe.

CVE ist ein eingetragenes Markenzeichen der MITRE Corporation.

Mozilla, Firefox und Thunderbird sind Markenzeichen der Mozilla Foundation in den USA und anderen Ländern.

Novell ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von Novell Enterprises Inc.

NetWare ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von Novell, Inc.

OpenVPN ist ein eingetragenes Markenzeichen von OpenVPN, Inc.

OpenSSL ist ein Markenzeichen der OpenSSL Software Foundation.

Oracle, Java, JavaScript und TouchDown sind eingetragene Markenzeichen von Oracle und/oder von verbundenen Unternehmen.

Parallels, das Parallels-Logo und Coherence sind Markenzeichen oder eingetragene Markenzeichen der Parallels International GmbH.

Chef ist ein Markenzeichen oder eingetragenes Markenzeichen der Progress Software Corporation und/oder einer ihrer Tochtergesellschaften oder verbundenen Unternehmen in den USA und/oder anderen Ländern.

Puppet ist ein Markenzeichen oder eingetragenes Markenzeichen von Puppet, Inc.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Red Hat, Fedora und Red Hat Enterprise Linux sind in den USA und in anderen Ländern Markenzeichen oder eingetragene Markenzeichen von Red Hat Inc oder seinen Tochtergesellschaften.

Ansible ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von Red Hat, Inc.

CentOS ist in den USA und in anderen Ländern ein Markenzeichen oder eingetragene Markenzeichen von Red Hat, Inc oder seinen Tochtergesellschaften.

BlackBerry steht im Besitz von Research In Motion Limited ist in den USA eingetragen. Die Marke kann auch in anderen Ländern angemeldet oder eingetragen sein.

Rocky Linux ist ein Markenzeichen der The Rocky Enterprise Software Foundation.

SAMSUNG ist ein eingetragenes Markenzeichen von SAMSUNG in den USA und anderen Ländern.

Debian ist ein eingetragenes Warenzeichen von Software in the Public Interest, Inc.

Splunk und SPL sind Markenzeichen und eingetragene Markenzeichen von Splunk Inc. in den USA und anderen Ländern.

SUSE ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von SUSE LLC.

Das Markenzeichen Symbian ist Eigentum der Symbian Foundation Ltd.

OpenAPI ist ein Markenzeichen von The Linux Foundation.

UNIX ist ein in den Vereinigten Staaten und in anderen Ländern eingetragenes Markenzeichen. Die Nutzung wird durch die Firma X/Open Company Limited lizenziert.

Zabbix ist ein eingetragenes Markenzeichen von Zabbix SIA.

Bekannte Probleme

Kaspersky Security Center Web Console hat eine Reihe von Einschränkungen, die für die Verwendung der Anwendung nicht kritisch sind:

- Änderungen an einem Aufgabenzeitplan werden nicht an verwaltete Geräte weitergegeben, wenn der Zeitplan die Einstellung **Nach Wochentagen** verwendet. Wenn Sie den Zeitplan ändern müssen, löschen Sie die vorhandene Aufgabe und erstellen Sie eine neue mit den aktualisierten Einstellungen.

- Wenn der Administrationsagent unter Microsoft Windows XP installiert ist, sind keine Informationen über verwaltete Anwendungskomponenten verfügbar.

- In der Konsole wird der Unterabschnitt **Alarme** im Abschnitt **Überwachung und Berichterstattung** des Hauptmenüs nur dann angezeigt, wenn Sie durch das Eingeben eines Aktivierungscodes einen EDR Optimum-Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzugefügt haben.

- Um die Verschlüsselungsstärke zu gewährleisten, muss das Zertifikat des Administrationsservers mit SHA-2 signiert sein und eine Schlüssellänge von mindestens 2048 besitzen. Wenn Sie das Zertifikat erneut ausstellen müssen, finden Sie Informationen dazu in der Wissensdatenbank von Kaspersky Security Center.

- Wenn Sie in Kaspersky Security Center 15.1 Web Console eine Aufgabe mit den **Zeitplaneinstellungen Alle N Tage** und Nach Wochentagen erstellen und die Aufgabe anschließend in einer früheren Version der Kaspersky Security Center Web Console oder Kaspersky Security Center Verwaltungskonsole öffnen (etwa wenn die Aufgabe auch auf sekundären Administrationsservern angewendet wird, die sowohl Linux-basierte als auch Windows-basierte Administrationsserver sein können), werden die Zeitplaneinstellungen möglicherweise falsch dargestellt, oder es kann ein Fehler auftreten.

- Wenn Sie in der Kaspersky Security Center Web Console den Export in ein SIEM-System konfigurieren und das UDP-Protokoll auswählen, wird nach dem Anklicken der Schaltfläche **Verbindung testen** ein Fehler ausgegeben. Die Ursache liegt darin, dass UDP keine Verbindung herstellt und das Übertragen der Daten kann nicht garantiert werden kann.

- Wenn Sie eine Aufgabe zur Deinstallation des Administrationsagenten auf einem Arm-Gerät mit mit Astra Linux Special Edition RUSB.10015-01 (Update 1.7) ausführen, wird der Administrationsagent erfolgreich entfernt, aber der in der Aufgabenliste angezeigte Aufgabenstatus mit dem aktuellen Fortschritt ist eingefroren.

- Das Eigenschaftenfenster der Richtlinie von Kaspersky Device Management für iOS enthält weiterhin den Abschnitt **Einstellungen für EAS-Geräte**, obwohl Exchange ActiveSync nicht mehr unterstützt wird.

- Das Herstellen einer HTTPS-Verbindung mit KSN schlägt fehl, wenn Kaspersky Center auf einem Gerät mit kyrillischen Symbolen im Gerätenamen installiert ist und der KSN-Proxy auf dem Administrationsserver aktiviert ist.

- Wenn Sie versuchen, die Eigenschaften eines Benutzerkontos zu ändern, für das die Option **Authentifizierung anfordern, um zu prüfen, ob Benutzerkonten geändert werden dürfen** aktiviert ist, und anschließend im Fenster **Schutz des Benutzerkontos** auf **Abbrechen** klicken, tritt ein unerwarteter Fehler auf.

- Wenn Sie auf Ihrem Gerät die Zeit oder die Zeitzone ändern, müssen Sie den Dienst der Kaspersky Security Center Web Console neu starten.

- Wenn auf dem Gerät ein Proxy verwendet wird und die Umgebungsvariablen des Proxys festgelegt sind, kann der Installer der Kaspersky Security Center Web Console einfrieren.

- Wenn Sie die Aufgabe *Download von Updates in die Datenverwaltungen der Verteilungspunkte* oder *Update-Prüfung* importieren, ist die Option **Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll** aktiviert. Diese Aufgaben können weder einer Geräteauswahl noch bestimmten Geräten zugewiesen werden. Wenn Sie die Aufgabe *Download von Updates in die Datenverwaltungen der Verteilungspunkte* oder *Update-Prüfung* bestimmten Geräten zuweisen, wird die Aufgabe fehlerhaft importiert.

- Wenn Sie eine Active Directory-Abfrage mit Linux-Verteilungspunkt mit installiertem Administrationsagenten Version 15 durchführen, können Sie nur Active Directory-Domänen abfragen, für die Sie die Adresse und die Anmeldeinformationen des Benutzers angeben. Die Abfrage der aktuellen Active Directory-Domäne und der Active Directory-Domänen-Gesamtstruktur ist nicht verfügbar.

- Nach dem Ausführen der Windows-Netzwerkabfrage werden möglicherweise Client-Geräte nicht gefunden.

- Wenn Sie im Assistenten zum **Hinzufügen eines sekundären Administrationsservers** ein Konto mit aktivierter zweistufiger Überprüfung auf dem zukünftigen sekundären Server angeben, wird der Assistent mit einem Fehler beendet. Um dieses Problem zu beheben, geben Sie ein Konto an, für das die zweistufige Überprüfung deaktiviert ist, oder erstellen Sie die Hierarchie vom zukünftigen sekundären Server.

- Wenn Sie sich bei der Kaspersky Security Center Web Console anmelden und dabei die Domänenauthentifizierung verwenden und einen virtuellen Administrationsserver für die Verbindung angeben, sich danach abmelden und anschließend versuchen, sich beim primären Administrationsserver anzumelden, stellt die Kaspersky Security Center Web Console eine Verbindung mit dem virtuellen Administrationsserver her. Um eine Verbindung mit dem primären Administrationsserver herzustellen, öffnen Sie den Browser erneut.

- Die schnelle oder vollständige Windows-Netzwerkabfrage liefert ein leeres Ergebnis zurück.

- Wenn Sie die Kaspersky Security Center Web Console mit der Identitäts- und Zugriffsverwaltung installieren und anschließend den Administrationsserver der Kaspersky Security Center Web Console ändern, erhält die Identitäts- und Zugriffsverwaltung keine Informationen über den neuen Administrationsserver.

- Ein verwaltetes Gerät, dass über mehr als einen Netzwerkadapter verfügt, übermittelt an den Administrationsserver die MAC-Adressinformationen von dem Netzwerkadapter, der nicht zum Herstellen der Verbindung mit dem Administrationsserver verwendet wird.

- Wenn für die Daten nicht das CEF-Format ausgewählt ist, schlägt die Test-Verbindung fehl.

- Die NTLM-Authentifizierung funktioniert nicht für Benutzerkonten innerhalb der Benutzergruppe "Geschützten Benutzer".