kaspersky

Kaspersky Next Expert View

© 2026 AO Kaspersky Lab

Inhalt

Online-Hilfe von Kaspersky Next Expert View

Neuerungen

Behobene Probleme

Kaspersky Next Expert View

- Hardware- und Softwarevoraussetzungen für Kaspersky Next Expert View
- Kompatible Anwendungen und Lösungen von Kaspersky
- Lokalisierung von Kaspersky Next Expert View
- Vergleich von Kaspersky Security Center und Kaspersky Next Expert View

Architektur und grundlegende Konzepte

- Architektur
- Von Kaspersky Next Expert View verwendete Ports
- Grundbegriffe
  - Administrationsagent
  - Administrationsgruppen
  - Hierarchie des Administrationsservers
  - Virtueller Administrationsserver
  - Verteilungspunkt
  - Web-Plug-ins zur Verwaltung
  - Richtlinien
  - Richtlinienprofile
  - Interaktion von Richtlinien und lokalen Programmeinstellungen

Lizenzierung des Programms

- Lizenzierung von Kaspersky Next Expert View
- Informationen über den Testmodus von Kaspersky Next Expert View
- Kaspersky Marketplace zum Finden von Kaspersky-Unternehmenslösungen verwenden
- Lizenzen und die Mindestanzahl von Geräten für jede Lizenz
- Ereignisse bei Überschreitung der Lizenzbeschränkung
- Methoden zur Verteilung von Aktivierungscodes an verwaltete Geräte
- Lizenzschlüssel des Administrationsservers hinzufügen
- Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
- Lizenzschlüssel auf Client-Geräte verteilen
- Lizenzschlüssel automatisch verteilen
- Informationen zu den verwendeten Lizenzschlüsseln in der Datenverwaltung des Administrationsservers anzeigen
- Informationen zu den Lizenzschlüsseln für ein bestimmtes Kaspersky-Programm anzeigen
- Lizenzschlüssel des Administrationsservers entfernen
- Lizenzschlüssel aus der Datenverwaltung entfernen
- Liste mit Geräten anzeigen, auf denen sich ein nicht aktiviertes Kaspersky-Programm befindet
- Vereinbarung mit einem Endbenutzer-Lizenzvertrag widerrufen
- Lizenzen für Kaspersky-Anwendungen verlängern
- Kaspersky Next Expert View nach Ablauf der Lizenz verwenden
- Lizenzdefinitionen
  - Über die Lizenz
  - Über das Lizenzzertifikat

- Über den Lizenzschlüssel
- Über den Aktivierungscode
- Über das Abonnement

Bereitstellung von Daten
- An Kaspersky-Server gesendete Daten
- Daten für den Betrieb von verwalteten Programmen
- Lokal verarbeitete Daten
- Über die rechtlichen Dokumente für Kaspersky Next Expert View

Härtungsleitfaden
- Die Architektur von Kaspersky Next Expert View planen
- Konten und Authentifizierung
- Verwaltung des Schutzes der Client-Geräte
- Konfigurieren des Schutzes für verwaltete Programme
- Ereignisübertragung an Systeme von Dritten
- Sicherheitsempfehlungen für Drittanbieter-Informationssysteme
- Empfehlungen für die Verwendung von Kaspersky-Sicherheitsanwendungen

Benutzeroberfläche von Kaspersky Next Expert View
- Sprache und Farbschema der Benutzeroberfläche ändern
- Startseite der Kaspersky Next Expert View anpassen
- Lesezeichen hinzufügen und entfernen
- Liste mit den Arbeitsbereichen abrufen

Erstkonfiguration von Kaspersky Next Expert View

Szenario: Erstellen einer Hierarchie von Administrationsservern, die durch Kaspersky Next Expert View verwaltet wird

Migration nach Kaspersky Next Expert View
- Methoden der Migration auf Kaspersky Next Expert View
- Szenario: Migration ohne Administrationsserver-Hierarchie
- Migrationsassistent
  - Schritt 1. Exportieren verwalteter Geräte, Objekte und Einstellungen aus Kaspersky Security Center Web Console
  - Schritt 2. Importieren der Exportdatei in Kaspersky Next Expert View
  - Schritt 3. Installieren Sie den Administrationsagenten erneut auf Geräten, die durch Kaspersky Next Expert View verwaltet werden
- Migration mit Hierarchie von Administrationsservern
- Szenario: Migration von Geräten mit Linux- oder macOS-Betriebssystem
- Szenario: Rückmigration von Kaspersky Next Expert View auf Kaspersky Security Center
- Migration mit virtuellen Administrationsservern
  - Szenario: Migration mit virtuellen Administrationsservern und durch Verschieben von Geräten
  - Szenario: Manuelle Migration mit virtuellen Administrationsservern
  - Szenario: Geräte aus Administrationsgruppen unter die Verwaltung von virtuellen Servern verschieben

Schnellstartassistent
- Über den Schnellstartassistenten
- Den Schnellstartassistent ausführen
- Schritt 1. Auswählen der herunterzuladenden Installationspakete
- Schritt 2. Konfigurieren eines Proxyservers
- Schritt 3. Kaspersky Security Network konfigurieren
- Schritt 4. Verwaltung der Updates von Drittherstellern konfigurieren
- Schritt 5. Erstellen einer grundlegenden Konfiguration für Netzwerkschutz
- Schritt 6. Schnellstartassistent abschließen

Erstbereitstellung von Kaspersky-Anwendungen
Szenario: Erstmalige Bereitstellung von Kaspersky-Programmen
Erstellen von Installationspaketen für Kaspersky-Programme
Installationspakete an sekundäre Administrationsserver verteilen
Erstellen eines autonomes Installationspakets für den Administrationsagenten
Liste der autonomen Installationspakete anzeigen
Erstellen benutzerdefinierter Installationspakete
Voraussetzungen für Verteilungspunkte
Einstellungen des Installationspakets des Administrationsagenten
Virtuelle Infrastruktur
Empfehlungen zur Senkung der Belastung auf den virtuellen Maschinen
Unterstützung von dynamischen virtuellen Maschinen
Unterstützung des Kopierens von virtuellen Maschinen
Administrationsagent für Windows, Linux und macOS: Vergleich
Einstellungen für die Remote-Installation auf Unix-Geräten angeben
Sicherheitsanwendungen von Drittanbietern ersetzen
Funktion zur manuellen Installation von Apps
Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Cloud Console
Assistent für die Bereitstellung des Schutzes
Schritt 1. Assistent für die Bereitstellung des Schutzes starten
Schritt 2. Installationspaket auswählen
Schritt 3. Auswählen der Version des Administrationsagenten
Schritt 4. Auswählen der Geräte
Schritt 5. Einstellungen für die Aufgabe zur Remote-Installation festlegen
Schritt 6. Verwaltung des Neustarts
Schritt 7. Deinstallieren inkompatibler Programme vor der Installation
Schritt 8. Verschieben von Geräten in die Gruppe "Verwaltete Geräte"
Schritt 9. Auswählen von Benutzerkonten für den Zugriff auf Geräten
Schritt 10. Beginnen der Installation
Netzwerkeinstellungen zur Interaktion mit externen Diensten
Ein Gerät auf dem Astra Linux im Modus der abgeschlossenen Softwareumgebung ausgeführt wird für die Installation des Administrationsagenten vorbereiten
Ein Linux-Gerät vorbereiten und den Administrationsagenten auf einem Linux-Gerät remote installieren
Programme mittels Aufgabe zur Remote-Installation installieren
Eine Anwendung remote installieren
Anwendungen auf sekundären Administrationsservern installieren
Kaspersky-Anwendungen starten und beenden
Verwaltung mobiler Geräte
Möglichkeiten von Detection and Response
Data Discovery
Über Data Discovery
Kategorien der Informationen, die Data Discovery finden kann
Data Discovery aktivieren
Die Bedingungen der Vereinbarung für Data Discovery akzeptieren
Verbinden einer Microsoft 365-Organisation mit Ihrem Arbeitsbereich
Anzeigen von Informationen über Funde von Data Discovery

Beispiel für die Analyse einer Erkennung von Data Discovery
Informationen über Funde von Data Discovery exportieren
Data Discovery deaktivieren
Geräte im Netzwerk suchen und Administrationsgruppen erstellen
Szenario: Netzwerkgeräte finden
Netzwerkabfrage
Windows-Netzwerkabfrage
Abfrage des Domänencontrollers
IP-Bereiche abfragen
Einen Samba-Domänencontroller konfigurieren
IP-Bereich hinzufügen und bearbeiten
Verteilungspunkte und Verbindungs-Gateways anpassen
Anzahl und Konfiguration der Verteilungspunkte bestimmen
Typische Konfiguration von Verteilungspunkten: Einzelbüro
Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros
Verteilungspunkte manuell zuweisen
Liste mit Verteilungspunkten für eine Administrationsgruppe bearbeiten
Verteilungspunkt als Push-Server verwenden
Verwenden der Option "Verbindung mit Administrationsserver nicht trennen" zur Bereitstellung einer dauerhaften Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver
Administrationsgruppen anlegen
Regeln für das Verschieben von Geräten erstellen
Regeln für das Verschieben von Geräten kopieren
Bedingungen für Verschiebungsregeln für Geräte
Geräte manuell zu einer Administrationsgruppe hinzufügen
Manuelles Verschieben von Geräten oder Clustern in eine Administrationsgruppe
Aufbewahrungsregeln für nicht zugeordnete Geräte anpassen
Arbeitsgerätebestand
Informationen über neue Geräte hinzufügen
Kriterien zur Erkennung von Unternehmensgeräten anpassen
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
Konfigurieren der Schutzeinstellungen für verwaltete Anwendungen
Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren
Aufgaben
Über Aufgaben
Über den Gültigkeitsbereich von Aufgaben
Aufgaben erstellen
Aufgabenliste anzeigen
Aufgaben manuell starten
Eine Aufgabe für ausgewählte Geräte starten
Allgemeine Einstellungen und Eigenschaften von Aufgaben

- Aufgaben exportieren
- Aufgaben importieren
- Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen

Client-Geräte verwalten

- Einstellungen eines verwalteten Geräts
- Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk
- Geräteauswahlen
  - Geräteliste einer Geräteauswahl anzeigen
  - Geräteauswahl erstellen
  - Einstellungen einer Geräteauswahl anpassen
  - Geräteliste einer Geräteauswahl exportieren
  - Geräte in der Auswahl aus Administrationsgruppen löschen
- Maßnahmen anzeigen und konfigurieren, wenn Geräte als inaktiv angezeigt werden
- Über die Varianten für den Gerätestatus
- Wechsel der Statuswerte von Geräten konfigurieren
- Den Administrationsserver für Client-Geräte ändern
- Konflikte zwischen mehreren Administrationsservern vermeiden
- Verbindungsprofile des Administrationsservers erstellen
- Über Cluster und Server-Arrays
- Eigenschaften eines Cluster- oder Server-Arrays
- Geräte-Tags
  - Geräte-Tag erstellen
  - Geräte-Tag umbenennen
  - Geräte-Tag löschen
  - Geräte mit zugewiesenen Tags anzeigen
  - Tags anzeigen, die einem Gerät zugewiesen sind
  - Tags manuell den Geräten zuweisen
  - Zugewiesene Tags von Geräten 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
- Quarantäne und Datei-Backups
  - Eine Datei aus der Datenverwaltung herunterladen
  - Dateien aus der Datenverwaltung entfernen
- 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
  - Systeminformationen von einem Client-Gerät herunterladen
  - Ereignisprotokolle downloaden
  - Starten, Stoppen und Neustarten der Anwendung
  - Ausführen der Ferndiagnose eines Programms und Herunterladen der Ergebnisse

Ausführen eines Programms auf einem Client-Gerät
Erzeugen einer Dump-Datei für eine Anwendung
Remotedesktopverbindung mit dem Client-Gerät herstellen
Verbindung mit den Client-Geräten über die Windows Desktopfreigabe herstellen
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
Administrationsgruppen verwalten
Administrationsgruppen anlegen
Programme automatisch auf Geräten einer Administrationsgruppe installieren
Administrationsgruppen verschieben
Deleting administration groups
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
Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren
Erzwungene Synchronisierung
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
Richtlinienprofil exportieren und importieren
Verschlüsselung und Datenschutz
Liste der verschlüsselten Laufwerke anzeigen
Verschlüsselungsberichte erstellen und anzeigen
Zugriff auf ein verschlüsseltes Laufwerk im autonomen Modus gewähren

- Benutzer und Benutzerrollen
  - Über Benutzerkonten
  - Benutzerkonto für einen internen Benutzer hinzufügen
  - Löschen eines Benutzerkontos eines internen Benutzers
  - Arbeitsbereichsadministratoren zuweisen
  - Über Benutzerrollen
  - Zugriffsrechte auf Anwendungsfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle
    - Zugriffsrechte auf Programmfunktionen
    - Vorkonfigurierte Benutzerrollen
    - Bestimmten Objekten Zugriffsrechte zuweisen
    - Zugriffsrechte an Benutzer und Sicherheitsgruppen zuweisen
  - Einem Benutzer oder einer Sicherheitsgruppe eine Rolle zuweisen
  - Benutzerrollen erstellen
  - Benutzerrollen bearbeiten
  - Gültigkeitsbereich einer Benutzerrolle bearbeiten
  - Benutzerrollen löschen
  - Richtlinienprofile mit Rollen verbinden
  - Eine Sicherheitsgruppe erstellen
  - Eine Sicherheitsgruppe bearbeiten
  - Benutzerkonten zu einer internen Gruppe hinzufügen
  - Löschen einer Sicherheitsgruppe
  - ADFS-Integration konfigurieren
  - Integration mit Microsoft Entra ID konfigurieren
    - Aktivieren der Microsoft Entra ID-Abfrage
    - Kaspersky Next Expert View zur Liste mit Programmen hinzufügen
  - Benutzer zu Gerätebesitzern ernennen
  - Benutzer nach der Installation des Administrationsagenten zum Linux-Gerätebesitzer ernennen
- Umgang mit Objekt-Revisionen
  - Hinzufügen einer Beschreibung der Revision
  - Objekte auf eine frühere Version zurück rollen
  - Revision einer Richtlinie anzeigen und speichern
  - Richtlinienrevisionen vergleichen
- Kaspersky Security Network (KSN)
  - Über KSN
  - KSN aktivieren und deaktivieren
  - Die akzeptierte KSN-Erklärung anzeigen
  - Eine aktualisierte KSN-Erklärung akzeptieren
  - Feststellen, ob der Verteilungspunkt als KSN-Proxyserver fungiert
- Objekte löschen

Datenbanken und Anwendungen von Kaspersky aktualisieren

- Szenario: Regelmäßige Aktualisierung der Kaspersky-Datenbanken und -Programme
- Über das Aktualisieren der Datenbanken, Software-Module und Programme von Kaspersky
- Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen
- Verwaltete Geräte so konfigurieren, dass Updates nur von Verteilungspunkten empfangen werden
- Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Next Expert View aktivieren und deaktivieren
- Automatische Installation von Updates für Kaspersky Endpoint Security für Windows

Informationen zum Update-Status
Programm-Updates genehmigen und ablehnen
Diff-Dateien zum Update von Kaspersky-Datenbanken und -Software-Modulen verwenden
Datenbanken und Software-Module von Kaspersky auf autonomen Geräten aktualisieren
Drittanbieter-Programme auf Client-Geräten verwalten
Einschränkungen des Schwachstellen- und Patch-Managements
Verfügbarkeit der Funktionen von Schwachstellen- und Patch-Management im Test- und kommerziellen Modus sowie unter verschiedenen Lizenzoptionen
Über Anwendungen von Drittanbietern
Updates für Drittanbieter-Programme
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
Drittanbieter-Anwendungen automatisch aktualisieren
Suchen und Schließen von Software-Schwachstellen
Beheben von Schwachstellen in Programmen
Erstellen der Aufgabe "Schwachstellen schließen"
Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen
Regeln für die Update-Installation hinzufügen
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
Szenario: Suchen und Schließen von Schwachstellen in Programmen
Die maximale Speicherdauer für Informationen über behobenen Schwachstellen festlegen
Verwalten des Programmstarts auf Client-Geräten
Programmkontrolle zur Verwaltung ausführbarer Dateien verwenden
Modi und Kategorien der Programmkontrolle
Liste der auf Client-Geräten installierten Anwendungen abrufen und anzeigen
Abrufen und Anzeigen einer Liste der auf Client-Geräten installierten ausführbaren Dateien
Erstellen einer manuell zu erweiternden Programmkategorie
Erstellen einer Programmkategorie mit ausführbaren Dateien aus ausgewählten Geräten
Liste der Programmkategorien anzeigen
Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows konfigurieren
Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen
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
- Administrationsserver konfigurieren
  - Hierarchie des Administrationsservers
  - Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen
  - Speicherdauer von Ereignissen für die gelöschten Geräte konfigurieren
  - E-Mails zu Ereignissen zusammenfassen
  - Einschränkungen bei der Verwaltung von sekundären Administrationsservern, die lokal über Kaspersky Next Expert View ausgeführt werden
  - Liste mit sekundären Administrationsservern anzeigen
  - Administrationsserver-Hierarchie löschen
  - Schnittstelle konfigurieren
  - Virtuelle Administrationsserver verwalten
    - Einen virtuellen Administrationsserver erstellen
    - Einen virtuellen Administrationsserver aktivieren und deaktivieren
    - Einem virtuellen Administrationsserver einen Administrator zuweisen
    - Einen virtuellen Administrationsserver 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 die Ereignisse in Kaspersky Next Expert View
Ereignisse von Kaspersky Next Expert View
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
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
Für Aufgaben und Richtlinien Informationen über Ereignisse protokollieren
Ereignisse löschen
Ereignisauswahl löschen
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
Über Benachrichtigungen
Anzeigen von Benachrichtigungen, die Ihre Aufmerksamkeit erfordern
Systembenachrichtigungen anzeigen
Anzeigen von Mitteilungen
Deaktivieren von Mitteilungen
Wechsel der Statuswerte von Geräten konfigurieren
Einstellungen für das Versenden von Benachrichtigungen anpassen
Erhalten von Warnungen bei Ablauf der Lizenz
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

Aktive Bedrohungen
Unverarbeitete Dateien desinfizieren
Unverarbeitete Dateien herunterladen
Dateien aus dem Abschnitt "Aktive Bedrohungen" löschen
Arbeiten mit Kaspersky Next Expert View unter der Lizenz für Kaspersky Next XDR Optimum
Integrationen für die Reaktion auf Alarme
Integration mit Active Directory für die Ausführung von Reaktionsmaßnahmen konfigurieren
Integration mit der Kaspersky Automated Security Awareness Platform konfigurieren
Integration mit Kaspersky Threat Intelligence Portal Sandbox konfigurieren
Alarme nach Attributen gruppieren
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
Systeminformationen von einem Client-Gerät herunterladen
Ereignisprotokolle downloaden
Starten, Stoppen und Neustarten der Anwendung
Ausführen der Ferndiagnose eines Programms und Herunterladen der Ergebnisse
Ausführen eines Programms auf einem Client-Gerät
Erzeugen einer Dump-Datei für eine Anwendung
Ferndiagnose auf einem Linux-basierten Client-Gerät ausführen
Ereignisse in SIEM-Systeme exportieren
Ereignisexport in SIEM-Systeme konfigurieren
Vorläufige Bedingungen
Über den Ereignisexport
Den Ereignisexport in ein SIEM-System konfigurieren
Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren
Ereignisse von Kaspersky-Anwendungen zum Export im Syslog-Format markieren
Allgemeine Ereignisse zum Export im Syslog-Format markieren
Über das Exportieren von Ereignissen im Syslog-Format
Konfiguration von Kaspersky Next Expert View für den Export an ein SIEM-System
Exportergebnisse anzeigen
Schnellstartanleitung für Managed Service Provider (MSP)
Über die Kaspersky Next Expert View
Hauptmerkmale von Kaspersky Next Expert View
Über die Lizenzierung der Kaspersky Next Expert View für Managed Service Provider (MSPs)
Informationen für MSPs zu den Funktionen für Detection and Response
Erste Schritte mit Kaspersky Next Expert View
Empfehlungen zur Verwaltung der Geräte Ihrer Kunden
Typisches Bereitstellungsschema für Managed Service Provider (MSPs)
Szenario: Bereitstellung des Schutzes (Verwaltung von Mandanten mittels virtueller Administrationsserver)
Szenario: Bereitstellung des Schutzes (Verwaltung von Mandanten mittels Administrationsgruppen)
Gemeinsame Verwendung von einem lokal ausgeführten Kaspersky Security Center und Kaspersky Next Expert View
Lizenzierung von Kaspersky-Programmen für Managed Service Provider (MSPs)
Überwachungs- und Berichtsfunktionen für Managed Service Provider (MSPs)

Arbeiten mit Kaspersky Next Expert View in einer Cloud-Umgebung
Varianten der Lizenzierung in der Cloud-Umgebung
Vorbereitung auf das Arbeiten in einer Cloud-Umgebung mittels Kaspersky Next Expert View
Arbeit mit der Cloud-Umgebung Amazon Web Services
Über die Arbeit in der Cloud-Umgebung Amazon Web Services
Erstellen von IAM-Benutzerkonten für Amazon EC2-Instances
Sicherstellen der Berechtigungen zur Arbeit der Kaspersky Next Expert View mit AWS
Erstellen eines IAM-Benutzerkontos für die Arbeit mit Kaspersky Next Expert View
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
Arbeiten mit Google Cloud
Der Assistent für das Konfigurieren der Cloud-Umgebung in Kaspersky Next Expert View
Schritt 1. Überprüfen der erforderlichen Plug-ins und Installationspakete
Schritt 2. Auswählen der Methode zur Programmaktivierung
Schritt 3. Auswählen der Cloud-Umgebung und Autorisierung
Schritt 4. Abfragen des Segments und Konfiguration der Synchronisierung mit der Cloud
Schritt 5. Konfiguration von Kaspersky Security Network für Kaspersky Next Expert View
Schritt 6. Erstellen einer Erstkonfiguration des Schutzes
Abfrage von Netzwerksegmenten mittels Kaspersky Next Expert View
Hinzufügen von Verbindungen für die Abfrage von Cloud-Segmenten über Kaspersky Next Expert View
Entfernen einer Verbindung für die Abfrage von Cloud-Segmenten
Konfiguration des Abfragezeitplans mittels Kaspersky Next Expert View anpassen
Anzeigen der Ergebnisse der Abfrage des Cloud-Segments durch Kaspersky Next Expert View
Anzeigen der Eigenschaften von Cloud-Geräten mittels Kaspersky Next Expert View
Synchronisation mit der Cloud: Konfigurieren der Verschiebungsregel
Remote-Installation von Programmen auf virtuellen Maschinen von Azure
Anfrage an den Technischen Support
Technischen Support erhalten
Technischer Support mit Kaspersky CompanyAccount
Hilfreiche Informationen für die Spezialisten des Technischen Supports von Kaspersky
Informationsquellen über das Programm
Bekannte Probleme
Glossar
Administrationsagent
Administrationsgruppe
Administrationsserver
Aktiver Schlüssel
Amazon EC2-Instance
Amazon Machine Image (AMI)
Antiviren-Datenbanken
Arbeitsbereich
Aufgabe
Aufgabe für eine Reihe von Geräten
Aufgabeneinstellungen
Authentifizierungsagent

AWS Application Program Interface (AWS API)

AWS IAM-Zugriffsschlüssel

AWS-Managementkonsole

Broadcast-Domäne

Cloud Discovery

Demilitarisierte Zone (DMZ)

Direkte Programmverwaltung

Ereignis-Datenverwaltung

Ereigniskategorie des Patches

Erzwungene Installation

Gerät mit Schutz auf UEFI-Ebene

Geräte-Tag

Gerätebesitzer

Grenzwert für Virenaktivität

Gruppenaufgabe

Gültigkeitsdauer der Lizenz

Home-Administrationsserver

HTTPS

IAM-Benutzer

IAM-Rolle

Identitäts- und Zugriffsverwaltung (IAM)

Inkompatibles Programm

Installationspaket

JavaScript

Kaspersky Next Expert View Administrator

Kaspersky Next Expert View Operator

Kaspersky Next Pro View

Kaspersky Private Security Network (KPSN)

Kaspersky Security Network (KSN)

Kaspersky-Update-Server

Konto in Kaspersky Next Expert View

Lightweight Nagent (LWNGT)

Lokale Aufgabe

Lokale Installation

Network Location Awareness (NLA)

Netzwerk-Antiviren-Schutz

Netzwerk-Schutzstatus

Programm-Tag

Programmeinstellungen

Push-Server

Quarantäne

Remote-Installation

Richtlinie

Richtlinienprofil

Schlüsseldatei

Schutzstatus

Schwachstelle

Signifikanz des Ereignisses
SSL
Update
Verbindungs-Gateway
Verfügbares Update
Verteilungspunkt
Verwaltetes Gerät
Virenangriff
Virtueller Administrationsserver
Web-Plug-ins zur Verwaltung
Wiederherstellung
Zentralisierte Programmverwaltung
Zusätzlicher Lizenzschlüssel (oder Reserve-Lizenzschlüssel)
Informationen über den Code von Drittherstellern
Markenrechtliche Hinweise

Online-Hilfe von Kaspersky Next Expert View

	**Neuerungen** Erfahren Sie, was in der aktuellsten Version der Anwendung neu ist.		**Netzwerkschutz konfigurieren** Verwalten Sie die Sicherheit einer Organisation durch das Konfigurieren von Richtlinien und Aufgaben für Kaspersky-Programme gemäß den Anforderungen der Organisation.
	**Hard- und Softwarevoraussetzungen** Überprüfen Sie, welche Betriebssysteme und Anwendungsversionen unterstützt werden.		**Kaspersky-Anwendungen: Regelmäßiges aktualisieren der Datenbanken und Anwendungsmodule** Sorgen Sie für die ununterbrochene Zuverlässigkeit des Schutzsystems.
	**Lizenzierung von Kaspersky Next Expert View** Erfahren Sie mehr über die Verwendung von Kaspersky Next Expert View im Testmodus und im kommerziellen Modus.		**Überwachung und Berichterstattung** Zeigen Sie Ihre Infrastruktur, den Schutzstatus von Netzwerkgeräten und die Statistiken an, um den aktuellen Schutzstatus Ihrer Organisation zu verwalten. Sie können auch Berichte verwenden.
	**Erstkonfiguration** Beginnen Sie die Arbeit mit Ihrem Arbeitsbereich, konfigurieren Sie Kaspersky Next Expert View nach Ihren Bedürfnissen.		**Schwachstellen- und Patch-Management** Schwachstellen in Programmen von Drittanbietern finden und schließen.
	**Migration nach Kaspersky Next Expert View** Migrieren Sie Ihre vorhandenen Administrationsgruppen und deren zugehörigen Objekte und Einstellungen von dem lokalen Kaspersky Security Center auf Kaspersky Next Expert View.		**Ereignisse in SIEM-Systeme exportieren** Konfigurieren Sie den Export von Ereignissen mittels Syslog-Protokoll in SIEM-Systeme.
	**Geräte im Netzwerk finden** Finden Sie vorhandene und neue Geräte im Netzwerk Ihres Unternehmens.		**Arbeiten in einer Cloud-Umgebung** Schützen Sie virtuelle Maschinen in den Cloud-Umgebungen von Amazon Web Services™, Microsoft Azure™ und Google™ Cloud Platform.
	**Verteilungspunkte und/oder Verbindungs-Gateways anpassen** Konfigurieren Sie die Verteilungspunkte.		**Die Funktionen von Kaspersky Next XDR Optimum in Kaspersky Next Expert View verwenden** Konfigurieren Sie die Integrationen, um auf Alarme zu reagieren, und fassen Sie Alarme zusammen, die zu einem Vorfall gehören, um den Untersuchungsprozess zu vereinfachen.
	**Kaspersky-Anwendungen: Zentralisierte Bereitstellung** Bereitstellung der Kaspersky-Anwendungen.		**Kurzanleitung für Managed Service Provider (MSPs)** Erfahren Sie, wie Sie Kaspersky Next Expert View einsetzen können, wenn Sie Administrator eines MSPs sind.

Neuerungen

Update vom August 2026

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Die Mitteilungszentrale ist jetzt verfügbar. Die Mitteilungszentrale zeigt Benachrichtigungen und Ankündigungen an, die Ihnen dabei helfen, über wichtige Ereignisse, Änderungen und Empfehlungen in Bezug auf Ihren Administrationsserver und die verwalteten Geräte informiert zu bleiben. Die Benachrichtigungen können in einer Tabelle gesucht, sortiert und gefiltert werden. Alle ungelesenen Benachrichtigungen können Sie schnell anzeigen, indem Sie auf das Mitteilungssymbol ( ) neben ihrem Benutzerkontomenü klicken.
- Optimierungen für mehr Benutzerfreundlichkeit:
  - Das Formular zum Akzeptieren der KSN-Erklärungen wurde überarbeitet: Um die KSN-Erklärung zu akzeptieren, müssen Sie jetzt die entsprechende Option auswählen.
  - Das Fenster **Neues benutzerdefiniertes Installationspaket** wurde geändert. Das Fenster enthält jetzt eine Funktion zum Datei-Upload. Wenn das benutzerdefinierte Installationspaket zu groß ist, wird vom System eine Fehlermeldung ausgegeben.
- Kaspersky Next Expert View unterstützt jetzt die Arbeit mit:
  - Kaspersky Endpoint Security 14.1 für Windows
  - Kaspersky Endpoint Security 12.5 für Linux

Update vom Juni 2026

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Sie können jetzt Administratoren mehreren virtuellen Servern gleichzeitig zuweisen.
- Sie können jetzt Arbeitsbereiche vom Testmodus in den kommerziellen Modus umschalten. Nach einem Wechsel wird der Arbeitsbereich nach Ablauf des 30-tägigen Testzeitraums nicht gelöscht.
- Im Abschnitt "Benutzer und Rollen" können Sie jetzt neue Benutzer zu Ihrem Arbeitsbereich hinzufügen. Sie können außerdem Arbeitsbereichen neue Benutzer als Administratoren zuweisen.
- Die Liste der Daten, die von Kaspersky Next beim Verbinden eines Geräts verarbeitet werden, wurde hinzugefügt.

- Erhöhte Benutzerfreundlichkeit:
  - Der Zuweisungsvorgang von Verteilungspunkten wurde verbessert: In der Liste werden jetzt nur noch nicht zugewiesene Verteilungspunkte angezeigt.
  - Der Algorithmus zur Erkennung von Geräten im Netzwerk wurde verbessert. Wenn die BIOS-Seriennummer, die Mainboard-Seriennummer, die IDs der Speichermedien oder die MAC-Adresse mit bereits bekannten Werten übereinstimmen, identifiziert der Administrationsserver ein Gerät nach einem Betriebssystem-Update oder einer Änderung der MAC-Adresse als bereits erkanntes Gerät.
  - Für den Abschnitt **Konsolen-Navigation** wurde das Layout zugunsten einer effektiveren Nutzung der Bildschirmfläche verbessert.
  - Die Lesbarkeit der Benachrichtigungsanzeige wurde in verschiedenen Systemszenarien verbessert.
- Kaspersky Next Expert View unterstützt die Arbeit mit:
  - Kaspersky Endpoint Security 14.0 für Windows
  - Kaspersky Embedded Systems Security 4.0 für Linux
  - Data Discovery: Erkennen Sie weitere Arten von sensiblen Daten und verhindern Sie die Weitergabe kritischer oder persönlicher Informationen
  - iOS MDM-Server: Verbinden Sie mobile iOS-Geräte mit dem Administrationsserver und verwalten Sie diese mittels Apple Push Notifications (APNs).

Update vom Februar 2026

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Verbesserte Benutzerfreundlichkeit:
  - Filterung von Client-Geräten nach Betriebssystemversion und Paketmanager umfasst nun auch Linux-Betriebssystemversionen.
  - Der Mechanismus zum Seitenumbruch für Tabellen in der Kaspersky Next Expert View wurde verbessert: Die Standardanzahl der angezeigten Elemente wurde auf 50 erhöht, und die benutzerdefinierte Anzahl der angezeigten Elemente bleibt nun zwischen den Sitzungen erhalten.
- Kaspersky Next Expert View unterstützt jetzt die folgenden Kaspersky-Programme:
  - Kaspersky Endpoint Security 12.12 für Windows
  - Kaspersky Endpoint Security 12.4 für Linux

- Der Administrationsagent unterstützt jetzt die Betriebssysteme der folgenden neuen Versionen:
  - CentOS Stream 10 64-Bit
  - Debian GNU/Linux 13 (Trixie) 64-Bit
  - Red Hat Enterprise Linux Server 10.x 64-Bit
- Die Infrastruktur von Kaspersky Next Expert View unterstützt jetzt die Lizenzen für Kaspersky Next XDR Ultimate.
- Sie können jetzt an Schulungen zur Cybersecurity teilnehmen, mit denen Sie zum Experten für IT-Sicherheit werden.

Update vom Oktober 2025

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Die Domänencontroller FreeIPA und ALD Pro werden unterstützt.
- Verbesserte Benutzerfreundlichkeit:
  - Die Navigation zwischen den Administrationsgruppen und Administrationsservern wurde vereinfacht: Sie können jetzt von einem einzigen Navigationsbereich aus zwischen den Gruppen und Servern wechseln.
  - Ihre Profileinstellungen werden in den oberen Bereich verschoben.
  - Die folgenden Abschnitte des Hauptmenüs wurden umbenannt:
    - Der Abschnitt **Assets (Geräte)** heißt jetzt **Asset-Verwaltung**.
    - Der Abschnitt **Verwaltete Geräte** heißt jetzt **Assets (Geräte)**.
    - **Direkt-Links** wurde in **Konsolen-Navigation** umbenannt.
  - Bei Bedarf kann das Hauptmenü auf Symbole minimiert werden.
- Die Filter, die Sie in den Abschnitten **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen** und **Vorgänge** → **Patch-Management** → **Software-Updates** auf Tabellen anwenden, wurden jetzt erfolgreich gespeichert und nicht zurückgesetzt.
- Kaspersky Next Expert View unterstützt jetzt die Arbeit mit:
  - Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit
  - Den folgenden Anwendungen von Kaspersky:
    - Kaspersky Endpoint Security 12.11 für Windows
    - Kaspersky Embedded Systems Security 4.0 für Windows

Update vom September 2025

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Wenn Sie den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum aktiviert und den Lizenzschlüssel für Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereitgestellt haben, können Sie Folgendes tun:
  - Alarme nach Attributen gruppieren.
  - Integrationen konfigurieren, um auf Bedrohungen zu reagieren.
- Wir haben den Begriff "Unternehmen" entfernt und es existieren nur noch "Arbeitsbereiche". Deshalb wurden Ihre bestehenden Arbeitsbereiche in das folgende Format umbenannt: `[ <Name_des_Unternehmens> ] <Name_des_Arbeitsbereichs>`.
- Die Kaspersky Security Center Cloud Console-Infrastruktur verfügt jetzt über die separate Registerkarte **Lizenzen**. Wenn eine Lizenz in mehreren Arbeitsbereichen verwendet wird, können Sie in der Registerkarte **Lizenzen** die Gesamtnutzung der Lizenz anzeigen.
- Ausgehend von der neuen Registerkarte **Lizenzen** können Sie auch aktuell gültigen Rechtsdokumente für Software-Lösungen und Sicherheitsanwendungen, die in Kaspersky Next Expert View verfügbar sind, anzeigen.
- Mithilfe spezieller Widgets und Banner in der Kaspersky Security Center Cloud Console-Infrastruktur können sich MSP-Administratoren (Managed Service Provider) jetzt einen Gesamtüberblick über die wichtigsten Status-Indikatoren aller ihrer Arbeitsbereiche verschaffen.

Update vom Juli 2025

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Es stehen jetzt Verbindungsprofile für mobile Benutzer mit Linux-Geräten zur Verfügung. Durch die Verwendung von Verbindungsprofilen können Sie die Regeln für Administrationsagenten auf Linux-Geräten so konfigurieren, dass diese je nach Gerätestandort eine Verbindung zum gleichen oder zu unterschiedlichen Administrationsservern herstellen.
- Es können jetzt Verschlüsselungsschlüssel zwischen Administrationsservern übertragen werden.
- Einige Versionen des Administrationsagenten werden nicht mehr unterstützt. Weitere Informationen erhalten Sie auf der Webseite mit den Produktlebenszyklen der Anwendungen. Aktualisieren Sie bei Bedarf Ihren Administrationsagenten auf eine Version mit **vollständigem** oder **eingeschränktem Support**-Status.
- Die Schaltfläche **Untersuchen** wurde aus dem Abschnitt **Quarantäne** entfernt.

- Kaspersky Next Expert View unterstützt jetzt die folgenden Kaspersky-Programme:
  - Kaspersky Endpoint Security 12.10 für Windows
  - Kaspersky Endpoint Security 12.3 für Linux
  - Kaspersky Endpoint Security 12.2 for Mac
- Die Benutzeroberfläche zum Anlegen und Verwalten von Arbeitsbereichen wurde verbessert.

Update vom April 2025

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt die folgenden Kaspersky-Programme:
  - Kaspersky Embedded Systems Security 3.4 für Linux
  - Kaspersky Endpoint Security 12.2 für Linux
  - Kaspersky Endpoint Security 12.8 für Windows
- Laden Sie eine Anwendung (oder ein Skript) zur Diagnose auf ein verwaltetes Gerät hoch und führen Sie es aus. Sie können jetzt sowohl den Ordner als auch das Archiv mit der ausführbaren Datei als auch die ausführbare Datei selbst hochladen. Nachdem die Anwendung erfolgreich ausgeführt wurde, können Sie die Ausführungsergebnisse herunterladen.
- Informationen über die Benutzer, die aktuell am verwalteten Gerät angemeldet sind, werden jetzt im Abschnitt **Allgemein** → **Sitzungen** des Fensters mit den Geräteeigenschaften angezeigt.
- Neue Sprachunterstützung: Die Infrastruktur von Kaspersky Next Expert View steht jetzt vollständig in chinesischer Sprache zur Verfügung.
- Verbesserte Benutzerfreundlichkeit:
  - Verfügbare Installationspakete werden auf einer Registerkarte angezeigt.
  - Sie können die Einstellungen der Startseite ändern, indem Sie den neuen Abschnitt **Quick-Links** verwenden. Standardmäßig ist die Registerkarte **Einstellungen der Startseite** des Abschnitts **Quick-Links** als Startseite festgelegt.
  - Die Navigation durch die Administrationsgruppen wurde aktualisiert: Sie können jetzt zu einer gewünschten Untergruppe gelangen, indem Sie im Pfad zur Administrationsgruppe auf den Link mit dem Gruppennamen klicken.
  - Der Abschnitt **Angeheftet** des Hauptmenüs heißt jetzt **Lesezeichen**. Sie können einzelne Abschnitte der Kaspersky Next Expert View zu den Lesezeichen hinzufügen, um schnell darauf zugreifen zu können.

Update vom Februar 2025

Dieses Update für Kaspersky Next Expert View verbessert die Leistung beim Öffnen der Web Console und beim Navigieren innerhalb der Web Console.

Update vom Oktober 2024

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Wir haben die Integration in Microsoft Entra ID verbessert. Wenn sich ein Benutzer jetzt von einem Microsoft Entra ID-Konto abmeldet, das für die Authentifizierung in Kaspersky Next Expert View verwendet wurde, wird die Sitzung auch für Kaspersky Next Expert View beendet und der Benutzer wird automatisch von der Konsole abgemeldet.
- Sie können jetzt Richtlinienänderungen anzeigen und herunterladen. Mit Kaspersky Next Expert View können Sie einen Bericht im HTML-Format ansehen oder die Revision in einer JSON-Datei speichern.
- Kaspersky Next Expert View zeigt nun den neuesten, dem Administrationsserver bekannten, Aufgabenstatus an.
- Der **Bericht über Netzwerkangriffe** beinhaltet jetzt die MAC-Adresse und den Port des angreifenden Geräts.
- Sie können nun die rechte Leiste schließen, indem Sie auf eine beliebige Stelle außerhalb der Leiste klicken. Wenn Sie Änderungen an der Leiste vornehmen und anschließend außerhalb der Leiste klicken, um diese zu schließen, erscheint ein Bestätigungsfenster.
- Die Tabellenüberschrift bleibt jetzt oben fixiert, wenn Sie durch die Tabelle blättern.

Update vom September 2024

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden Verbesserungen:

- Kaspersky Endpoint Agent 4.0 wird unterstützt.
- Einige alte Versionen verschiedener Browser werden nicht mehr unterstützt (Chrome bis 128, Edge bis 128, Firefox ESR bis 115 und Safari bis 17.6).

Update vom April 2024

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Eine neue Funktion für Cloud Discovery. Mit dieser Funktion können Sie die Verwendung von Cloud-Diensten auf verwalteten Windows-Geräten überwachen und den Zugriff auf unerwünschte Cloud-Dienste blockieren. Cloud Discovery überwacht die Zugriffsversuche von Benutzern auf diese Dienste sowohl über Browser als auch über Desktop-Anwendungen.

- Integration mit Microsoft Entra ID, damit sich die Benutzer in Ihrem Unternehmen mit deren Anmeldedaten von Microsoft Entra ID an der Kaspersky Next Expert View anmelden können. Beachten Sie, dass diese Funktion in der Russischen Föderation nicht verfügbar ist.

- Sie können jetzt Profile für die Verbindung des Administrationsagenten mit dem Administrationsserver erstellen. Die Verbindungsprofile erlauben mobilen Benutzern mit Laptops die Verbindungsmethode mit dem Administrationsserver zu ändern oder abhängig von aktuellen Standort des Geräts im Netzwerk zwischen Administrationsservern umzuschalten.

- Sie können jetzt direkt aus dem Hauptmenü des Programms die Liste Ihrer Arbeitsbereiche öffnen.

- Es wurden zwei weitere Sprachen hinzugefügt: Chinesisch (traditionell) und Chinesisch (vereinfacht).

- In den Aufgabeneinstellungen wurde für das Speichern von Ereignissen die Standardeinstellung von **Alle Ereignisse speichern** auf **Nur die Ergebnisse der Aufgabenausführung speichern** geändert. Diese Option reduziert den benötigten Speicherplatz für die Datenbank des Arbeitsbereichs. Die Änderung betrifft nur Aufgaben, die für Kaspersky Security Center erstellt wurden. Diese Einstellung bleibt in den Aufgaben für Kaspersky-Sicherheitsanwendungen unverändert.

- Kaspersky Next Expert View informiert Sie jetzt zusätzlich über die geplante Löschung Ihres Arbeitsbereiches 7 Tage und 30 Tage nachdem der letzte Lizenzschlüssel aus dem Arbeitsbereich gelöscht wurde oder abgelaufen ist. Dadurch steht Ihnen mehr Zeit zur Verfügung, um einen andere Lizenz zu erwerben und deren Lizenzschlüssel zum Arbeitsbereich hinzuzufügen.

- Sowohl Kaspersky Business Hub als auch die Infrastruktur von Kaspersky Next Expert View unterstützen jetzt die folgenden Lizenzen für Kaspersky Next: Das Logo der Anwendung ändert sich automatisch entsprechend der von Ihnen verwendeten Lizenz.

- Kaspersky Next Expert View unterstützt jetzt die folgenden Kaspersky-Anwendungen:

  - Kaspersky Endpoint Security für Windows Version 12.4

  - Kaspersky Endpoint Security 12.0 für Mac Patch A

- Wenn Sie von einer Kaspersky-Sicherheitsanwendung auf eine andere migrieren möchten und die aktuelle Anwendung durch ein Kennwort geschützt ist, können Sie das Kennwort für die Deinstallation direkt in den Eigenschaften der Aufgabe zur Remote-Installationsaufgabe angeben.

- Sie können jetzt das Hauptmenü der Anwendung anpassen, indem Sie Ihre bevorzugten Menüabschnitte anheften oder loslösen. Die angehefteten Abschnitte werden für den schnellen Zugriff zum Bereich **Angeheftet** hinzugefügt.

- In den Startzeitplan-Einstellungen von Aufgaben wurde für die Option **Nach Abschluss einer anderen Aufgabe** die Benutzeroberfläche und das Benutzererlebnis optimiert.

- Der Bericht zur Hardware kann jetzt Informationen über macOS-Geräte aufnehmen.
- Sie können jetzt mehrere Client-Geräte aus der Geräteliste auswählen und für diese anschließend eine zuvor erstellte Aufgabe starten.

Update vom Februar 2024

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Aus der Liste der verwalteten Geräte können Sie jetzt ein Gerät oder mehrere Geräte auswählen und ihm oder ihnen anschließend eine vorhandene Aufgabe zur Ausführung zuweisen. Die aktuelle Geräte im Gültigkeitsbereich der Aufgabe werden durch die von Ihnen ausgewählten Geräte ersetzt.
- Sie können jetzt Geräte-Tags mehreren Geräten gleichzeitig zuweisen oder Geräte-Tags von mehreren Geräten gleichzeitig entfernen. Wählen Sie dazu aus der Liste der verwalteten Geräte die Geräte aus und geben Sie anschließend die Tags an, die Sie den ausgewählten Geräten zuweisen oder von ihnen entfernen möchten.
- Verbesserte Darstellung und Benutzerführung für die Liste der verwalteten Geräte. Die neue Spalte **Tags** wurde hinzugefügt und die Geräte können nach Geräte-Tags gefiltert werden.

Update vom Januar 2024

Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 12.4 für Windows.

Update vom Dezember 2023

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Sie können jetzt die Verbindungsherstellung mit SIEM-Systemen testen.
- Kaspersky Next Expert View unterstützt jetzt die Abfrage von Microsoft Active Directory-Domänencontrollern und Samba-Domänencontrollern mithilfe von Linux-Verteilungspunkten.
- Remote-Diagnose von verwalteten Linux-Geräten.
- Kaspersky Security Center Cloud Console unterstützt jetzt die folgenden Kaspersky-Anwendungen:
  - Kaspersky Endpoint Security für Windows Version 12.3 Patch A
  - Kaspersky Endpoint Security 12.0 für Linux
  - Kaspersky Endpoint Security 12.0 für Mac
  - Kaspersky Endpoint Agent 3.16
  - Kaspersky Embedded Systems Security 3.3 für Windows

- Zwei Abschnitte der Benutzeroberfläche wurden aus dem Hauptmenü ausgeblendet, da sie nicht zum Funktionsumfang des Programms gehören:
  - Verschlüsselungsereignisse (**Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselungsereignisse**)
  - IP-Bereiche (**Gerätesuche und Bereitstellung** → **Gerätesuche** → **IP-Bereiche**)
- Wir haben den Inhalt der Vereinbarung zum Datenschutz für Kaspersky Next Expert View aktualisiert.
- Einige ältere Browser-Versionen werden nicht mehr unterstützt (Firefox ESR vor Version 102).

Update vom September 2023

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt Kaspersky Embedded Systems Security 3.3 für Linux.
- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 12.2 für Windows.
- Optimierung der Benutzeroberfläche beim Arbeiten mit der Benutzerliste im Abschnitt **Asset-Verwaltung**.

Update vom Juni 2023

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Ein neuer Härtungsleitfaden wurde veröffentlicht. Wir empfehlen Ihnen dringend, den Leitfaden sorgfältig zu lesen und die Sicherheitsempfehlungen zu befolgen, um Kaspersky Next Expert View und Ihre Netzwerkinfrastruktur zu konfigurieren.
- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 11.3 für Mac.
- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 11.4 für Linux.
- Darüber hinaus stehen Ihnen in Kaspersky Next Expert View folgende Funktionen zur Verfügung: Export von Ereignisauswahlen in eine Datei, und anschließender Import der Ereignisauswahlen in Kaspersky Security Center Windows oder Kaspersky Security Center Linux.
- Sie können jetzt einen Verteilungspunkt als Push-Server für die vom Administrationsagenten verwalteten Geräte verwenden. Mit dieser Funktion können Sie sicherstellen, dass zwischen einem verwalteten Gerät und dem Administrationsserver eine kontinuierliche Verbindung besteht.
- Neuorganisation des Abschnitts mit den Einstellungen zur Integration Kaspersky Next Expert View mit anderen Kaspersky-Anwendungen.
- Neuorganisation der Benutzeroberfläche des Abschnitts **Remote-Diagnose**.

- Sie können jetzt mit einem Mal die Informationen zu allen Geräten in einer csv-Datei speichern, die in einer Geräteauswahl enthalten sind.

- Eine Reihe von Verbesserungen an der Benutzeroberfläche und der Benutzerfreundlichkeit, einschließlich der Möglichkeit, alle Elemente in einer Tabelle auszuwählen.

Update vom März 2023

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt Cluster und Server-Arrays als verwaltete Geräte. Wenn eine Kaspersky-Anwendung auf einem Cluster-Knoten installiert ist, sendet der Administrationsagent diese Informationen an den Administrationsserver. In der Web Console werden Cluster und Server-Arrays getrennt von anderen verwalteten Geräten aufgelistet. Jeden Cluster oder Server-Array wird als einzelnes, untrennbares Objekt verwaltet.

- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 12.0 für Windows.

- Die maximale Anzahl an Einträgen, die ein Bericht enthalten kann, wurde für Berichte in der Web Console auf bis zu 2.500 und für Berichte, die in eine Datei exportiert werden auf bis 10.000 erhöht.

- Sie können jetzt auswählen, ob Sie im Bericht über den Schutzstatus die verwalteten Geräte mit dem Status *OK* aufnehmen möchten.

- Sie können Kaspersky Next Expert View jetzt aktivieren, indem Sie eine der folgenden Lizenzen verwenden oder Lizenzschlüssel der aufgeführten Lizenzen einem vorhandenen Arbeitsbereich hinzufügen:

  - Kaspersky Symphony Security

  - Kaspersky Symphony EDR

  - Kaspersky Symphony MDR

  - Kaspersky Symphony XDR

- Eine spezielle Version des Administrationsagenten für Windows XP wurde veröffentlicht.

- Der aktualisierte Administrationsagent für Linux unterstützt den KSN Proxy-Service. Neben Windows-basierten Verteilungspunkten können Sie jetzt Linux-basierte Verteilungspunkte verwenden, um Anfragen an Kaspersky Security Network (KSN) von den verwalteten Geräten weiterzuleiten. Diese Option erlaubt Ihnen die Umverteilung und Optimierung des Datenverkehrs im Netzwerk.

- Der aktualisierte Administrationsagent für Linux unterstützt die Funktion Programm-Registry. Der Administrationsagent kann eine Liste der auf dem Linux-basierten verwalteten Gerät installierten Programme zusammenstellen und diese Liste anschließend an den Administrationsserver weiterleiten.

- Darüber hinaus stehen Ihnen in Kaspersky Next Expert View 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.

Update vom November 2022

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 11.3 für Linux.
- Kaspersky Next Expert View unterstützt jetzt Kaspersky Managed Detection and Response 2.1.18.
- Um macOS 13 zu unterstützen, unterstützt Kaspersky Next Expert View jetzt aktualisierte Versionen von Kaspersky Endpoint Security for Mac 11.2 und 11.2.1.
- Die Videos im Abschnitt **Tutorials** wurden aktualisiert.

Update vom Oktober 2022

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Wir haben den Inhalt der Vereinbarung zum Datenschutz für Kaspersky Next Expert View aktualisiert.
- Die Infrastruktur der Kaspersky Next Expert View benachrichtigt Sie jetzt über einen Arbeitsbereich, der keinen aktiven Lizenzschlüssel besitzt und der möglicherweise gelöscht wird, wenn Sie keinen neuen Lizenzschlüssel hinzufügen.
- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 11.11.0 für Windows.
- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Detection and Response Optimum 2.3.
- Kaspersky Embedded Systems Security 3.2 für Windows wird unterstützt.

Update vom September 2022

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Sie können jetzt spezielle Administratoren für virtuelle Administrationsserver zuweisen. Dafür erstellen Sie ein Administrator-Benutzerkonto und gewähren dem Administrator die Zugriffsrechte für den virtuellen Administrationsserver. Der zugewiesene Administrator hat nur Zugriff auf den ausgewählten virtuellen Administrationsserver und kann sich nicht mit dem primären Administrationsserver oder anderen sekundären Administrationsservern (physischen oder virtuellen) verbinden.
- Die Benutzererfahrung beim Löschen eines Lizenzschlüssels für die Kaspersky Next Expert View wurde optimiert. Der neue Mechanismus verhindert, dass Sie versehentlich Ihren letzten aktiven Lizenzschlüssel löschen.
- Sie können jetzt Verteilungspunkte auf Linux-Basis verwenden, um mittels der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* die Antiviren-Datenbanken für die Sicherheitsanwendungen von Kaspersky herunterzuladen.

- Der Administrationsagent ist jetzt in japanischer Lokalisierung verfügbar.
- In der Benutzeroberfläche der Kaspersky Next Expert View wurden die in Großbuchstaben ausgeschriebenen Abschnittsnamen an die gewöhnliche Groß- und Kleinschreibung angepasst.

Update vom August 2022

Neue Sprachunterstützung: Kaspersky Next Expert View steht jetzt vollständig in japanischer Sprache zur Verfügung.

Update vom Juli 2022

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Unterstützung der folgenden neuen Versionen von Kaspersky-Anwendungen:
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 für Mac
  - Kaspersky Security für iOS: 1.0.0
  - Kaspersky Endpoint Security 11.10.0 für Windows
- Wir haben die Inhalte der Vereinbarung zum Datenschutz und der Vereinbarung für Kaspersky Next Expert View aktualisiert.
- Zusätzliche Sprachunterstützung: Die Infrastruktur von Kaspersky Next Expert View ist jetzt in Japanisch verfügbar. Die Sprachunterstützung für Japanisch innerhalb der Arbeitsbereiche von Kaspersky Next Expert View folgt demnächst.

Update vom April 2022

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 11.9.0 für Windows.
- Kaspersky Next Expert View unterstützt jetzt die japanische Lokalisierung von Kaspersky Embedded Systems Security.

Update vom 9. März 2022

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Die Integration mit Kaspersky Endpoint Detection and Response Expert wurde implementiert.
- Die Incident Response Platform (IRP) wurde implementiert. Sie können jetzt Sicherheitsvorfälle über die Kaspersky Next Expert View verwalten.
- Kaspersky Next Expert View akzeptiert jetzt Lizenzschlüssel für Kaspersky Endpoint Detection and Response Expert. Die Mindestanzahl an Geräten für die Lizenz beträgt 50.

Update vom 11. Februar 2022

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Die Lizenzen von Kaspersky Embedded Systems Security für Windows werden jetzt unterstützt.
- Kaspersky Endpoint Security 11.8.0 für Windows wird unterstützt.
- Kaspersky Endpoint Security 11.8.0 für Windows kann aus einem Programmpaket in japanischer Sprache installiert werden.
- Kaspersky Endpoint Agent 3.12 wird unterstützt.

Update vom 10. Dezember 2021

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Das Arbeiten mit den internen Benutzern wurde verbessert:
  - Sie können dem Portal jetzt neue interne Benutzer hinzufügen.
  - Das Programm bewahrt Sie davor, aus Versehen Ihre eigenen Rechte herabzusetzen.

Update vom 18. Oktober 2021

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Detection and Response Optimum 2.0.
- Sie können jetzt mobile Android-Geräte mithilfe der Kaspersky Next Expert View verwalten.

- Der Kaspersky Marketplace ist als neuer Menüeintrag verfügbar: Sie können jetzt direkt in der Kaspersky Next Expert View nach neuen Kaspersky-Anwendungen suchen.

- Im Menü steht ein neuer Abschnitt namens Mitteilungen von Kaspersky zur Verfügung. Die Mitteilungen von Kaspersky informieren Sie über Wissenswertes zu den Kaspersky-Anwendungen, die auf Ihren verwalteten Geräten installiert sind. Die Informationen in diesem Abschnitt werden durch die Kaspersky Next Expert View regelmäßig aktualisiert.

- Sie können jetzt sekundäre Administrationsserver, die mit Linux betrieben werden, über die Kaspersky Next Expert View verwalten.

Update vom 7. September 2021

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Sie können jetzt Active Directory Federation Services (AD FS) verwenden, um sich unter Verwendung Ihres Active Directory-Benutzerkontos an Kaspersky Next Expert View anzumelden. Es muss kein neues Benutzerkonto mehr angelegt werden.

- Kaspersky Next Expert View arbeitet jetzt mit folgenden Cloud-Umgebungen: Amazon Web Services, Microsoft Azure und Google Cloud. Um virtuelle Maschinen (oder Instanzen) in einer Cloud-Umgebung zu schützen, benötigen Sie eine der Lizenzen von Kaspersky Hybrid Cloud Security. Der Assistent für das Konfigurieren der Cloud-Umgebung ist verfügbar.

- Die Maximalanzahl der Geräte pro Arbeitsbereich beträgt jetzt 25.000.

- Die Integration in SIEM-Systeme ist jetzt in Kaspersky Next Expert View verfügbar. Sie können unter Verwendung des Syslog-Protokolls Ereignisse an SIEM-Systeme exportieren.

- Sie können jetzt virtuelle Administrationsserver erstellen. Jeder virtuelle Administrationsserver kann über seine eigene Struktur von Administrationsgruppen, Richtlinien, Aufgaben, Berichten und Ereignissen verfügen. Sie können den virtuellen Administrationsserver für die Verwaltung von Kundenunternehmen mit komplexen Arbeitsabläufen innerhalb Ihres Arbeitsbereichs verwenden. Sie können jedoch keine virtuellen Administrationsserver von einem lokal ausgeführten Kaspersky Security Center in Kaspersky Next Expert View migrieren.

- Sie können jetzt in Tabellen die Breite der Spalten anpassen, die Tabellen sortieren und nach Daten durchsuchen.

- Wir haben die Stabilität und Verfügbarkeit von Kaspersky Business Hub und Kaspersky Next Expert View verbessert.

Update vom 27. Oktober 2020

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Security 11.6.0 für Windows, Kaspersky Endpoint Security 11.1 für Mac Patch A und Kaspersky Endpoint Agent 3.10 (als Teil von Kaspersky Endpoint Detection and Response Optimum).
- Sie können jetzt folgende Lizenzen verwenden:
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Endpoint Security for Business Advanced
  - Kaspersky Total Security for Business
- Es sind folgende Funktionen enthalten:
  - Schwachstellen- und Patch-Management
  - Verschlüsselungsverwaltung
  - Programmkontrolle
  - Adaptive Kontrolle von Anomalien
  - RDP-Sitzungen, inklusive Windows Desktopfreigabe
- Das Navigationsmenü ist jetzt vertikal angeordnet und ähnelt damit der Benutzeroberfläche von Kaspersky Security Center auf Basis der Microsoft Management Console.
- Es stehen jetzt Lehrvideos für ein technisches Training zur Verfügung. Diese unterstützen Sie beim Kennenlernen der Funktionsweise des Programms.

Update vom 30. Juni 2020

Dieses Update von Kaspersky Next Expert View beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Next Expert View unterstützt jetzt Kaspersky Security 11 für Windows Server (beginnend ab September 2020).
- Kaspersky Next Expert View unterstützt jetzt Kaspersky Endpoint Agent 3.9 und Kaspersky Endpoint Security 11.4.0 für Windows.
- Der Schnellstartassistent wurde verbessert: Einige Schritte wurden entfernt, die Reihenfolge der Schritte wurde leicht geändert und einige Texte wurden für mehr Bedienungsfreundlichkeit überarbeitet.
- Kaspersky Next Expert View ist jetzt in italienischer Sprache verfügbar.

- Sie können jetzt den Endbenutzer-Lizenzvertrag (EULA) für jede verwaltete Kaspersky-Anwendung über die Benutzeroberfläche von Kaspersky Next Expert View widerrufen. Vor dem Widerruf der EULA müssen Sie das ausgewählte Programm deinstallieren.

- Sie können jetzt Arbeitsbereiche löschen. Wenn Sie einen Arbeitsbereich für die Löschung markieren, wird dieser standardmäßig nach sieben Tagen automatisch gelöscht. Sie können die Löschung des Arbeitsbereiches jedoch auch erzwingen, so dass dieser sofort gelöscht wird.

- Für das Anmelden an der Konsole wurde die zweistufige Überprüfung implementiert.

Behobene Probleme

Die folgende Tabelle enthält alle Probleme, die in früheren Updates von Kaspersky Next Expert View gefunden und in der aktuellen Version behoben wurden.

Liste der in Kaspersky Next Expert View behobenen Probleme

Kaspersky Next Expert View-Update, in dem das Problem erstmals aufgetreten ist	Problem-ID	Problembeschreibung
Update vom Februar 2026	9526104	Es wurde ein Problem behoben, durch das der QuickInfo-Text mit dem Hintergrund verschmolz, wenn Sie Mobilgerät-Zertifikate auswählten.
Update vom Juni 2026	9577592	Es wurde ein Problem behoben, durch das bei umfangreichen Richtlinien von Kaspersky Endpoint Security der Abschnitt **Anwendungseinstellungen** möglicherweise nicht richtig geladen wurde und daher leer erschien.
Update vom Juni 2026	10065748	Es wurde ein Problem behoben, durch das beim Anzeigen des Berichts **Bericht über die Web-Kontrolle** in der Web Console keine detaillierten Informationen zu einer Regel angezeigt wurden, wenn deren Name eckige Klammern enthielt.
Update vom Juni 2026	10112458	Es wurde ein Problem behoben, durch das unter **Einschränkungen des Testmodus** im Abschnitt **Einschränkungen für Anwendungsfunktionen** Informationen zu Beschränkungen für Installationspakete fehlten.
Update vom Juni 2026	10117987	Es wurde ein Problem behoben, durch das der Abschnitt **Administrationsserver** im Hauptmenü in allen nicht englischsprachigen Lokalisierungen auf Englisch angezeigt wurde.
Update vom Juni 2026	10128693	Es wurde ein Problem behoben, das beim Speichern einer Richtlinie nach dem Vornehmen von Änderungen zur Meldung „**Ein Fehler ist aufgetreten**“ führte.
Update vom Juni 2026	10128748	Es wurde ein Problem behoben, durch das in der Anwendungsliste beim Erstellen der Aufgabe **Anwendung starten/beenden** falsche Anwendungen des Unified Protection and Management Plug-ins angezeigt wurden.
Update vom Juni 2026	10183311	Es wurde ein Problem behoben, durch das die Aufgabe **Suche nach Schwachstellen und erforderlichen Updates** möglicherweise mit dem Status **Abgeschlossen mit Warnung** abgeschlossen wurde.
Update vom Juni 2026	10189276	Es wurde ein Problem behoben, durch das eine festgelegte Beschränkung für die Anzahl der Sicherheitsgruppen möglicherweise nicht ordnungsgemäß eingehalten wurde.
Update vom Juni 2026	10189594	Es wurde ein Problem behoben, durch das der Abschnitt **Dashboard** zusammen mit der Hierarchie der Administrationsgruppen falsch angezeigt wurde, wenn Sie durch manuelles Ändern der URL in der Adressleiste des Browsers vom Abschnitt **Dashboard** zum Abschnitt **Aufgaben** navigierten.
Update vom Februar 2026	9501104	Es wurde ein Problem behoben, durch das Tutorials im entsprechenden Abschnitt möglicherweise beim ersten Versuch nicht gestartet werden konnten.
Update vom Juni 2026	9968154	Es wurde ein Problem behoben, durch das Benachrichtigungen möglicherweise in der falschen Sprache angezeigt wurden, nachdem die Sprache der Web Console-Schnittstelle geändert worden war.
Update vom Juni 2026	10076008	Es wurde ein Problem behoben, durch das beim Navigieren zwischen Abschnitten während des Ladens der Seite möglicherweise kurzzeitig das helle Design anstelle des dunklen Designs angezeigt wurde.
Update vom Juni 2026	10076016	Es wurde ein Problem behoben, durch das ein Benutzer, dem die entsprechenden Berechtigungen gerade erst entzogen worden waren, weiterhin einen Bericht mit aktuellen Daten zu vorhandenen Lizenzen herunterladen konnte.
Update vom Juni 2026	10112524	Es wurde ein Problem behoben, durch das nach dem Wechsel der Lokalisierung ein unnötiger `ui_locales`-Parameter in der URL angezeigt wurde.
Update vom Juni 2026	10126364	Es wurde ein Problem behoben, durch das Sie von einer kommerziellen Lizenz zu einer Demolizenz wechseln konnten.

Update vom Juni 2026	10128638	Es wurde ein Problem behoben, durch das ein Benutzer im Abschnitt **Benutzer und Rollen → Rollen** möglicherweise nicht korrekt angezeigt wurde, nachdem ihm in den Eigenschaften der Administrationsgruppe benutzerdefinierte Berechtigungen zugewiesen worden waren.
Update vom Juni 2026	10146377	Es wurde ein Problem behoben, durch das der MDR-Bereich, wenn er als Startseite festgelegt war, auch nach der Deaktivierung der Option **Funktionen von MDR anzeigen** im Abschnitt **Einstellungen → Einstellungen der Benutzeroberfläche** die Startseite blieb.
Update vom Juni 2026	10157485	Es wurde ein Problem behoben, durch das Daten aus dem Abschnitt **Schwachstellen in Programmen** nicht korrekt in die Formate CSV und TXT exportiert wurden.

Kaspersky Next Expert View

Kaspersky Next Expert View ist für Administratoren von Unternehmensnetzwerken und für Mitarbeiter, die für die Sicherheit von Geräten in Unternehmen verantwortlich sind, gedacht. Es bietet umfangreiche Optionen zum Schutz Ihrer Benutzergeräte und wird für große Unternehmen empfohlen. Kaspersky Next Expert View wird durch Kaspersky gehostet und gewartet. Sie müssen Kaspersky Next Expert View nicht auf Ihrem Computer oder Server installieren.

Mit Kaspersky Next Expert View können Sie Folgendes tun:

- Kaspersky-Anwendungen auf Geräten Ihres Netzwerks installieren und die installierten Anwendungen verwalten.
- Eine Hierarchie der Administrationsgruppen erstellen, um eine Gruppe von bestimmten Client-Geräten als Ganzes zu verwalten.
- Virtuelle Administrationsserver erstellen und in einer Hierarchie arrangieren.
- Ihre Netzwerkgeräte schützen, einschließlich Workstations und Server:
  - Ein auf Kaspersky-Anwendungen basierendes System für Schutz vor Malware verwalten.
  - Die Fähigkeiten von Detection and Response (EDR und MDR) nutzen (für Kaspersky Endpoint Detection and Response und/oder Kaspersky Managed Detection and Response wird eine Lizenz benötigt), einschließlich:
    - Analysieren und Untersuchen von Vorfällen
    - Visualisieren von Vorfällen durch das Erstellen eines Diagramms mit der Entwicklungskette der Bedrohung
    - Annehmen oder ablehnen von Reaktionen, sowie Aktivieren von Auto-Akzeptieren für alle Reaktionen
- Kaspersky Next Expert View als mandantenfähige Anwendung verwenden.
- Kaspersky-Anwendungen, die auf Client-Geräten installiert sind, remote verwalten.
- Die zentrale Bereitstellung von Lizenzschlüsseln für Kaspersky-Anwendungen auf Client-Geräten durchführen.
- Sicherheitsrichtlinien für Geräte in Ihrem Netzwerk erstellen und verwalten.
- Benutzerkonten erstellen und verwalten.
- Benutzerrollen erstellen und verwalten (RBAC).
- Aufgaben für Programme, die auf Ihren Netzwerkgeräten installiert sind, erstellen und verwalten.
- Für jedes Kundenunternehmen separate Berichte zum Status des jeweiligen Sicherheitssystems anzeigen.

Bevor Sie Kaspersky Next Expert View verwenden können, müssen Sie ein Benutzerkonto erstellen und einen Arbeitsbereich anlegen.

Sie verwalten Kaspersky Next Expert View mithilfe der Web Console, welche die Interaktion zwischen Ihrem Gerät und dem Administrationsserver über einen Browser sicherstellt. Beim Administrationsserver handelt es sich um eine Anwendung, das für die Verwaltung der auf Ihren Netzwerkgeräten installierten Kaspersky-Anwendungen konzipiert ist. Wenn Sie mithilfe Ihres Browsers eine Verbindung zur Kaspersky Next Expert View herstellen, stellt der Browser eine sichere Verbindung mit dem Server von Kaspersky Next Expert View her.

Der Administrationsserver und das verbundene Datenbankverwaltungssystem (DBMS) werden Ihnen in einer Cloud-Umgebung als Dienst bereitgestellt. Wartung und Pflege des Administrationsservers und des DBMS werden als Teil des Dienstes bereitgestellt. Alle Programmkomponenten von Kaspersky Next Expert View werden aktuell gehalten. Vom Administrationsserver und den erstellten Objekten (wie Richtlinien und Aufgaben) werden regelmäßig Sicherungskopien angelegt, um deren Schutz zu erhöhen.

Kaspersky Next Expert View ist eine mehrsprachige Anwendung. Sie können die Sprache der Benutzeroberfläche jederzeit und ohne erneutes Öffnen der Anwendung ändern.

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.

Hardware- und Softwarevoraussetzungen für Kaspersky Next Expert View

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.

Verwaltungskonsole

Für die Nutzung von Kaspersky Next Expert View auf einem Client ist nur ein Browser erforderlich.

Für die Arbeit mit Kaspersky Next Expert View kann nur ein einziges Browserfenster oder eine einzelne Registerkarte verwendet werden.

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 Next Expert View verwendet wird.

Browser:

- Google Chrome 145.0.7632.26 oder höher
- Microsoft Edge 145.0.3800.65 oder höher
- Safari 18.6 auf macOS
- Mozilla Firefox Extended Support Release 140.7.1.2 oder höher

Administrationsagent

Hardwaremindestvoraussetzungen:

- CPU mit einer 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.

Mindestvoraussetzungen an die Hardware für Schwachstellen und Patch-Management:

- CPU mit einer Taktfrequenz von 1.4 GHz oder höher. Ein 64-Bit-Betriebssystem ist erforderlich.
- RAM: 8 GB.

- Freier Speicherplatz auf dem Datenträger: 1 GB.

Vom Administrationsagenten unterstützte Betriebssysteme

Betriebssysteme. Workstations mit Microsoft Windows	Microsoft Windows Embedded POSReady 2009 mit dem aktuellsten Service Pack, 32-Bit Microsoft Windows Embedded 7 Standard mit Service Pack 1 32-Bit/64-Bit Microsoft Windows Embedded 8.1 Industry Pro 32-Bit/64-Bit Microsoft Windows 10 Enterprise 2015 LTSB 32-Bit/64-Bit Microsoft Windows 10 Enterprise 2016 LTSB 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-Bit/64-Bit Microsoft Windows 10 Enterprise 2019 LTSC 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise Version 1703, 1709, 1803, 1809 32-Bit/64-Bit Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise Version 1909 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise LTSC 2021 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise Version 1607 32-Bit/64-Bit Microsoft Windows 10 TH1 (Juli 2015) Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS4 (Update vom April 2018, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS5 (Oktober 2018) Home/Profi/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS6 (Mai 2019) Home/Profi/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 20H1 (Update vom Mai 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 20H2 (Update vom Oktober 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 20H1 (Update vom Mai 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 21H2 (Update vom Oktober 2021) Home/Pro/Pro für Workstations/Enterprise/Bildung 32-Bit/64-Bit Microsoft Windows 10 22H2 (Update vom Oktober 2023) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 8.1 Pro/Enterprise 32-Bit/64-Bit Microsoft Windows 8 Pro/Enterprise 32-Bit/64-Bit Microsoft Windows 7 Home/Pro/Enterprise/Ultimate mit Service Pack 1 und höher, 32-Bit/64-Bit Microsoft Windows XP Professional mit Service Pack 3 und höher, 32-Bit (unterstützt vom Administrationsagenten in Version 14.0.0.20023; erfordert das Sicherheitsupdate für Windows XP KB2868626) Microsoft Windows XP Professional for Embedded Systems mit Service Pack 3 32-Bit (unterstützt vom Administrationsagenten in Version 14.0.0.20023)

Betriebssysteme. Server mit Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-Bit Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Foundation mit Service Pack 2 32-Bit/64-Bit Microsoft Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation mit Service Pack 1 und höher, 64-Bit Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-Bit Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-Bit Microsoft Windows Server 2016 Server Core/Datacenter/Essentials/Standard (Installationsoption) (LTSB) 64-Bit Microsoft Windows Server 2019 Standard/Datacenter/Core 64-Bit Microsoft Windows Server 2019 RS5 Essentials/Standard 64-Bit Microsoft Windows Server 2022 Standard/Datacenter/Core 64-Bit Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-Bit Microsoft Windows Server 2025 Standard/Datacenter/Core 64-Bit Microsoft Windows Small Business Server 2011 Standard/Essentials/Premium Add-on 64-Bit
Betriebssysteme. Linux	Debian GNU/Linux 13 (Trixie) 64-Bit Debian GNU/Linux 12 (Bookworm) 32-Bit/64-Bit Debian GNU/Linux 11.x (Bullseye) 32-Bit/64-Bit Ubuntu Server 24.04 LTS 64-Bit Ubuntu Server 22.04 LTS 64-Bit Ubuntu Server 20.04 LTS (Focal Fossa) 64-Bit CentOS 7.x 64-Bit CentOS Stream 10 64-Bit CentOS Stream 9 64-Bit CentOS Stream 8 64-Bit Red Hat Enterprise Linux Server 10.x 64-Bit Red Hat Enterprise Linux Server 9.x 64-Bit Red Hat Enterprise Linux Server 8.x 64-Bit Red Hat Enterprise Linux Server 7.x 64-Bit openSUSE Leap 15 64-Bit SUSE Linux Enterprise Server 15 (alle Service Packs) 64-Bit SUSE Linux Enterprise Server 12 (alle Service Packs) 64-Bit Oracle Linux 7 64-Bit Oracle Linux 8 64-Bit Oracle Linux 9 64-Bit Linux Mint 21.x 64-Bit Linux Mint 22.x 64-Bit Alma Linux 8.x 64-Bit Alma Linux 9.x 64-Bit Rocky Linux 8.x 64-Bit Rocky Linux 9.x 64-Bit Amazon Linux 2 64-Bit Kylin 10 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.

Ausführliche Informationen zu den unterstützten Virtualisierungsplattformen finden Sie in der Online-Hilfe zu Kaspersky Security for Virtualization Light Agent.

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

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).

Kompatible Programme und Lösungen von Kaspersky

Lizenzen für verschiedene Produkte gewähren verschiedene Konstellationen von Anwendungen und Lösungen von Kaspersky.

Die folgenden Anwendungen und Lösungen von Kaspersky können Sie über die Kaspersky Next Expert View bereitstellen und verwalten:

- Kaspersky Endpoint Security 14.1 für Windows (nur mit Unterstützung für Lite-Verschlüsselung (AES56))
- Kaspersky Endpoint Security 12.5 für Linux
- Kaspersky Endpoint Security 12.2 for Mac
- Kaspersky Embedded Systems Security 4.0 für Windows
- Kaspersky Embedded Systems Security 4.0 für Linux
- Kaspersky Endpoint Agent 4.0
- Kaspersky Endpoint Security für Android
- Kaspersky Security für iOS

Die folgenden Lösungen können Sie integrieren, um Sicherheitsvorfälle anzuzeigen und zu bearbeiten:

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Endpoint Detection and Response Expert

- Kaspersky Next XDR Expert
- Kaspersky Next XDR Optimum

Wenn Sie eine neue Programmversion auf einem verwalteten Gerät installieren, jedoch eine veraltete Richtlinie für die neue Programmversion verwenden, anstatt die Richtlinie zu aktualisieren, stellt das Programm weiterhin Daten für Kaspersky Next Expert View bereit. Kaspersky Next Expert View kann diese Daten jedoch nicht verarbeiten wie im Abschnitt Durch verwaltete Anwendungen verarbeitete Daten der Dokumentation beschrieben. Damit Kaspersky Next Expert View diese Daten verarbeiten kann, müssen Sie für die neue Programmversion eine neue Richtlinie erstellen.

Lokalisierung von Kaspersky Next Expert View

Die Benutzeroberfläche und Dokumentation von Kaspersky Next Expert View sind in folgenden Sprachen verfügbar:

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

Vergleich von Kaspersky Security Center und Kaspersky Next Expert View

Sie können Kaspersky Security Center auf folgende Arten verwenden:

- Als Cloud-Lösung

  Kaspersky Security Center ist für Sie in einer Cloud-Umgebung installiert und Kaspersky gewährt Ihnen den Zugriff auf den Administrationsserver in Form eines Dienstes. Sie verwalten die Netzwerksicherheit durch eine cloudbasierte Verwaltungskonsole namens Kaspersky Next Expert View. Die Benutzeroberfläche dieser Konsole ist ähnlich der von Kaspersky Security Center Web Console.

- Als On-Premises-Lösung (Windows- oder Linux-basiert)

  Sie installieren Kaspersky Security Center auf einem lokalen Gerät und verwalten die Netzwerksicherheit entweder durch die auf der Microsoft Management Console basierenden Verwaltungskonsole oder durch die Kaspersky Security Center Web Console.

  Neben dem Windows-basierten Programm steht Kaspersky Security Center Linux auch für Linux zur Verfügung. Kaspersky Security Center Linux wurde entwickelt, um den Schutz von Linux-Geräten bereitzustellen und zu verwalten, indem ein Linux-basierter Administrationsserver verwendet wird, um die Anforderungen von reinen Linux-Umgebungen zu erfüllen. Kaspersky Security Center für Windows und Kaspersky Security Center Linux unterscheiden sich in ihrem Funktionsumfang.

In der folgenden Tabelle können Sie die wichtigsten Funktionen von Kaspersky Security Center und Kaspersky Next Expert View vergleichen.

Funktionsvergleich von Kaspersky Security Center on-premises und als Cloud-Lösung

Funktion oder Eigenschaft	Kaspersky Security Center wird on-premise ausgeführt	Kaspersky Next Expert View
Standort des Administrationsservers	On-premises	Cloud
Standort des Datenbankmanagementsystems (DBMS)	On-premises	Cloud
Web-basierte Verwaltungskonsole	✓	✓
Wartung von Administrationsserver und DBMS	Durch den Kunden	Durch Kaspersky
Hierarchie des Administrationsservers	✓	✓ (Der Administrationsserver von Kaspersky Next Expert View kann nur als primärer Administrationsserver in der Hierarchie fungieren und kann nur zur Überwachung von Richtlinien und Aufgaben verwendet werden.)
Hierarchie der Administrationsgruppen	✓	✓
Migration der verwalteten Geräte und zugehörigen Objekte von Kaspersky Security Center on-premises zur Kaspersky Next Expert View	✓	✓
Netzwerkabfrage	✓	✓ (nur mittels Verteilungspunkten)
Maximale Anzahl verwalteter Geräte	100.000	25.000
Schutz von verwalteten Windows-, Linux- und macOS-Geräten	✓	✓
Schutz von mobilen Geräten	✓	✓ (es werden nur Kaspersky Endpoint Security für Android und Kaspersky Security für iOS unterstützt)

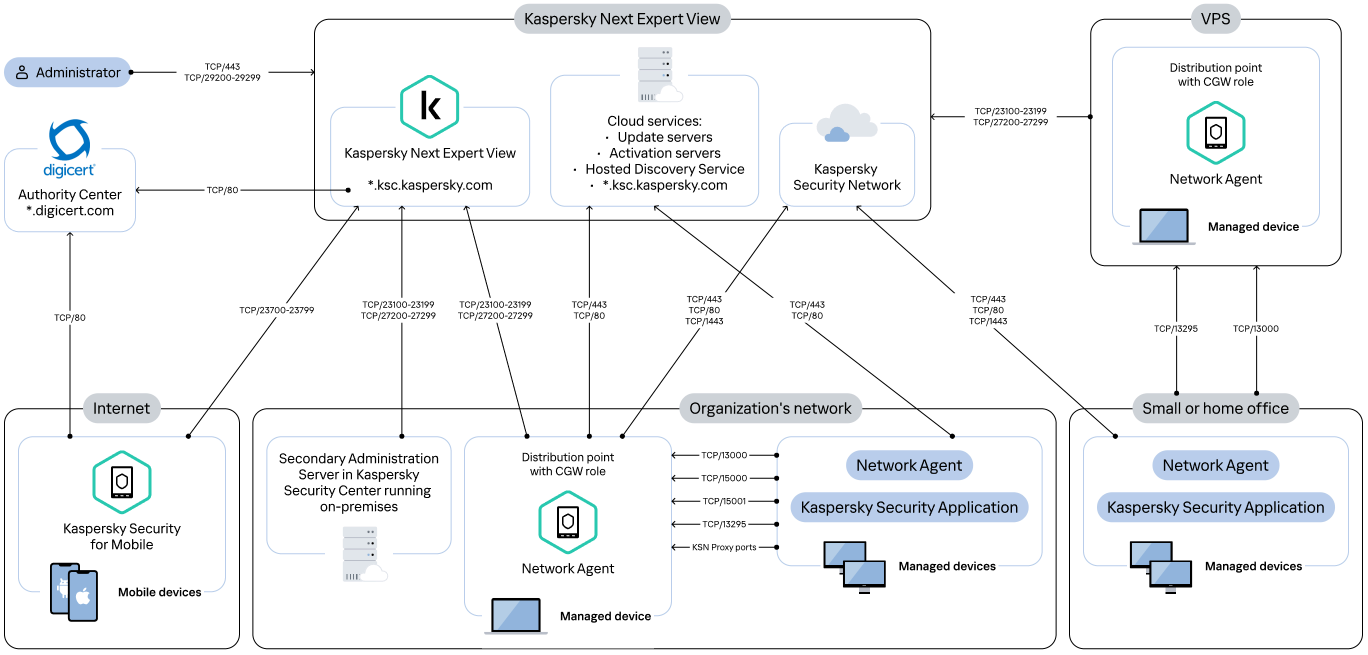
Funktion oder Eigenschaft	Kaspersky Security Center wird on-premise ausgeführt	Kaspersky Next Expert View
Schutz der Public-Cloud-Infrastruktur	✓	✓
Gerätezentrierte Sicherheitsverwaltung	✓	✓
Anwendungsrichtlinien	✓	✓
Aufgaben für Kaspersky-Anwendungen	✓	✓
Kaspersky Security Network	✓	✓
KSN-Proxyserver	✓	✓ (nur auf Verteilungspunkten)
Kaspersky Private Security Network	✓	—
Zentralisierte Bereitstellung von Lizenzschlüsseln für Kaspersky-Anwendungen	✓	✓
Wechseln verwalteter Geräte auf einen anderen Administrationsserver	✓	— (Um verwaltete Geräte zu einem anderen Administrationsserver zu wechseln, müssen Sie auf den Geräten den Administrationsagenten neu installieren.)
Unterstützung für virtuelle Administrationsserver	✓	✓
Updates für Drittanbieter-Programme installieren und Schwachstellen in Drittanbietern-Programmen schließen	✓	✓ (Um Sicherheitslücken in den Drittanbieter-Programmen zu beheben, können nur empfohlene Patches installiert werden.)
Benachrichtigungen über Ereignisse auf verwalteten Geräten	✓	✓
Erstellen und Verwalten von Benutzerkonten	✓	✓
Maximale Anzahl an Ereignissen in der Datenbank	400.000 (kann auf bis zu 45.000.000 erhöht werden)	400.000
Integration von SIEM-Systemen	✓	✓ (nur mittels Syslog-Format und des TLS over TCP-Protokolls)
Verwendung des Administrationsservers als WSUS-Server	✓	—
Überwachen der Statuswerte von Richtlinien und Aufgaben	✓	✓
Unterstützung von Clustern und Server-Arrays in Verwaltungsgruppen	✓	✓
Remote-Installation von Betriebssystemen	✓	—
SNMP-Unterstützung	✓	—
Maximale Anzahl der virtuellen Server	500	200
Festplatte eines Geräts klonen	✓	—
Unterstützung von OpenAPI	✓	—

Architektur und grundlegende Konzepte

In diesem Abschnitt werden die Anwendungsarchitektur und die grundlegenden Konzepte von Kaspersky Next Expert View erläutert.

Architektur

Dieser Abschnitt enthält eine Beschreibung der Komponenten von Kaspersky Next Expert View und deren Interaktion.



Kaspersky Next Expert View-Architektur

Das durch die cloudbasierte Konsole verwaltete Kaspersky Next Expert View besitzt zwei Hauptkomponenten: Die Infrastruktur von Kaspersky Next Expert View und die Infrastruktur des Kunden.

Die Infrastruktur von Kaspersky Next Expert View umfasst:

- **Cloudbasierte Verwaltungskonsole**. Bietet eine Weboberfläche zum Erstellen und Verwalten des Schutzsystems in dem von Kaspersky Next Expert View verwalteten Netzwerk des Kundenunternehmens.
- **Cloud-Dienste**. Umfassen Update- und Aktivierungsserver.
- **Kaspersky Security Network (KSN)**. Server, die eine Datenbank von Kaspersky mit fortlaufend 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.

Die Infrastruktur des Kunden umfasst:

- **Verteilungspunkt**. Computer, auf dem der Administrationsagent installiert ist und der zur Update-Verteilung, Netzwerkabfrage, Remote-Installation von Programmen und zum Empfangen von Informationen über Computer in einer Administrationsgruppe und/oder Broadcasting-Domäne verwendet wird. Der Administrator wählt die entsprechenden Geräte aus und weist sie manuell als Verteilungspunkte zu. Verteilungspunkte können auch als Verbindungs-Gateways fungieren, um die Anzahl ausgehender externer Verbindungen sowie die Anzahl gleichzeitiger Verbindungen zum Administrationsserver zu reduzieren. Es wird empfohlen, die Anzahl der verwalteten Computer zu begrenzen, die sich direkt mit dem Administrationsserver verbinden.

- **Verwaltete Geräte**. Computer im Netzwerk des Kunden, die durch Kaspersky Next Expert View geschützt werden. Auf jedem verwalteten Gerät muss ein Administrationsagent und eine Kaspersky-Sicherheitsanwendungen installiert sein.

- **Lokal ausgeführte sekundäre Administrationsserver** (optional). Sie können lokal ausgeführte Administrationsserver verwenden, um eine Hierarchie von Administrationsservern zu erstellen.

Von Kaspersky Next Expert View verwendete Ports

Um Kaspersky Next Expert View als Teil der Kaspersky Infrastruktur zu verwenden, müssen Sie auf den Client-Geräten die folgenden Ports öffnen, um eine Internetverbindung zu gewährleisten (siehe untere Tabelle):

Ports, die auf Client-Geräten geöffnet werden müssen, um eine Internetverbindung zu gewährleisten

Port (oder Portbereich)	Protokoll	Zweck des Ports (oder Portbereichs)
23100-23199	TCP/TLS	Empfangen von Verbindungen von Administrationsagenten und sekundären Administrationsservern auf dem Administrationsserver der Kaspersky Next Expert View unter *.ksc.kaspersky.com. Die Kaspersky-Infrastruktur kann jeden Port innerhalb dieses Bereichs und jede beliebige Webadresse innerhalb dieser Maske verwenden. Der Port und die Web-Adresse können sich mit der Zeit ändern.
23700 – 23799 (nur wenn Sie mobile Geräte verwalten)	TCP/TLS	Annehmen von Verbindungen von mobilen Geräten. Verbindung zum Administrationsserver der Kaspersky Next Expert View unter *.ksc.kaspersky.com. Die Kaspersky-Infrastruktur kann jeden Port innerhalb dieses Bereichs und jede beliebige Webadresse innerhalb dieser Maske verwenden. Der Port und die Web-Adresse können sich mit der Zeit ändern.
27200 – 27299	TCP/TLS	Annehmen von Verbindungen von verwalteten Geräten (mit Ausnahme mobiler Geräte) zur Programmaktivierung. Verbindung zum Administrationsserver der Kaspersky Next Expert View unter *.ksc.kaspersky.com. Die Kaspersky-Infrastruktur kann jeden Port innerhalb dieses Bereichs und jede beliebige Webadresse innerhalb dieser Maske verwenden. Der Port und die Web-Adresse können sich mit der Zeit ändern.
29200 – 29299	TCP/TLS	Tunneln von Verbindungen zu verwalteten Geräten mithilfe des Tools "klsctunnel" über den Administrationsserver der Kaspersky Next Expert View unter *.ksc.kaspersky.com. Die Kaspersky-Infrastruktur kann jeden Port innerhalb dieses Bereichs und jede beliebige Webadresse innerhalb dieser Maske verwenden. Der Port und die Web-Adresse können sich mit der Zeit ändern.
443	HTTPS	Verbindung mit dem Kaspersky Next Expert View Discovery Service unter *.ksc.kaspersky.com. Sämtliche Webadressen innerhalb dieser Maske können von der Kaspersky-Infrastruktur verwendet werden.
1443	TCP	Verbindung mit Kaspersky Security Network
80	TCP	Die Verbindung wird verwendet, um auf *.digicert.com die Gültigkeit der Zertifikate von Kaspersky Security Center zu überprüfen. Sämtliche Webadressen innerhalb dieser Maske können von der Kaspersky-Infrastruktur verwendet werden.

Die folgende Tabelle listet die Ports auf, die auf Client-Geräten mit installiertem Administrationsagenten geöffnet sein müssen.

Ports, die auf Client-Geräten geöffnet werden müssen

Portnummer	Protokoll	Zweck des Ports	Gültigkeitsbereich
15000	UDP	Empfangen von Daten des Verbindungs-Gateways (falls verwendet)	Verwaltung von Client-Geräten
15000	UDP-Broadcast	Erhalten von Daten anderer Administrationsagenten, die sich in der gleichen Broadcast-Domäne befinden	Zustellung von Updates und Installationspaketen
15001	UDP	Empfangen von Multicast-Anfragen von einem Verteilungspunkt (falls verwendet)	Empfang von Updates und Installationspaketen von einem Verteilungspunkt

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 Next Expert View 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 Client-Geräten mit installiertem Administrationsagent, welcher als Verteilungspunkt fungiert, geöffnet sein müssen.

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

Portnummer	Protokoll	Zweck des Ports	Gültigkeitsbereich
13000	TCP/TLS	Annahme der Verbindungen von den Administrationsagenten	Verwaltung der Client-Geräte und Zustellung von Updates und Installationspaketen
13111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	TCP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver
13295 (nur wenn Sie den Verteilungspunkt als Push-Server verwenden)	TCP/TLS	Versand von Push-Benachrichtigungen an verwaltete Geräte	Verwendung eines Verteilungspunkts als Push-Server
15111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	UDP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver
17111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	HTTPS	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver

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.

Wenn Sie in Ihrem Netzwerk einen oder mehrere Administrationsserver als sekundäre Administrationsserver einsetzen, während sich der primäre Administrationsserver innerhalb der Kaspersky-Infrastruktur befindet, beachten Sie bitte die Liste der Ports, die von Kaspersky Security Center und einem lokal ausgeführten Kaspersky Security Center Linux verwendet werden. Nutzen Sie diese Ports für die Interaktion zwischen Ihrem sekundären Administrationsserver (oder Ihren sekundären Administrationsservern) und den Client-Geräten.

Grundbegriffe

Dieser Abschnitt enthält ausführliche Definitionen der Grundbegriffe zu Kaspersky Next Expert View.

Administrationsagent

Interaktion zwischen dem Administrationsserver und den Geräten wird mithilfe der Komponente *Administrationsagent* von Kaspersky Next Expert View durchgeführt. Der Administrationsagent muss auf allen Geräten installiert werden, auf welchen Kaspersky-Anwendungen mittels Kaspersky Next Expert View 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 beim 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.

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

Der Administrationsagent synchronisiert das verwaltete Gerät mit dem Administrationsserver. Kaspersky Next Expert View synchronisiert den Administrationsserver mehrmals pro Stunde automatisch mit den verwalteten Geräten. Der Administrationsserver legt das Synchronisierungsintervall (auch als *Heartbeat* bezeichnet) in Abhängigkeit von der Anzahl der verwalteten Geräte fest.

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 Next Expert View 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 den Computer dieses Mitarbeiters von der Administrationsgruppe "Buchhalter" in die Administrationsgruppe "Entwickler" verschieben. Danach erhält der Computer automatisch die Programmeinstellungen, die für Entwickler erforderlich sind.

Hierarchie des Administrationsservers

Administrationsserver können eine primär-/sekundär-Hierarchie bilden. Jeder Administrationsserver kann über mehrere sekundäre Administrationsserver auf verschiedenen Hierarchieebenen verfügen. Die Tiefe der Verschachtelung ist für sekundäre Administrationsserver nicht beschränkt. Zu den Administrationsgruppen des primären Administrationsservers gehören die Client-Geräte aller sekundärer Administrationsserver.

Der Administrationsserver von Kaspersky Next Expert View kann ausschließlich als primärer Administrationsserver fungieren und kann als sekundärer Server ausschließlich lokal ausgeführte Administrationsserver besitzen.

Bei der Migration von dem lokal ausgeführten Administrationsserver auf einen Administrationsserver von Kaspersky Next Expert View können Sie die Administrationsserver in einer Hierarchie arrangieren. Um die Migration anschließend schrittweise durchzuführen, können Sie einen Teil Ihrer verwalteten Geräte unter die Verwaltung des Administrationsservers von Kaspersky Next Expert View stellen. Die restlichen verwalteten Geräte können unter Verwaltung des lokal ausgeführten Administrationsservers verbleiben. Dies erlaubt es Ihnen, die Verwaltungsfunktionen von Kaspersky Next Expert View auf einer ausgewählten Anzahl von verwalteten Geräten zu testen. Gleichzeitig können Sie Richtlinien, Aufgaben, Berichte und andere Objekte konfigurieren, um die Verwaltung und Überwachung Ihres gesamten Netzwerks zu testen. Dies erlaubt es Ihnen bei Bedarf zu den Objekten zurückzukehren, die auf dem lokal ausgeführten Administrationsserver konfiguriert waren.

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. Verwenden Sie in den Administrationsgruppen der verschiedenen Administrationsserver die Funktion zur Suche nach Geräten unter Berücksichtigung der Netzwerkattribute.

Virtueller Administrationsserver

Ein virtueller Administrationsserver (im Folgenden auch *Virtueller Server* genannt) ist eine Komponente des Programms Kaspersky Next Expert View, die dazu konzipiert ist, den Antiviren-Schutz im Netzwerk eines Kundenunternehmens zu verwalten. Jeder virtuelle Administrationsserver kann über seine eigene Struktur von Administrationsgruppen und über seine eigenen Mittel zur Verwaltung und Überwachung, wie Richtlinien, Berichte und Ereignisse, verfügen. Der funktionelle Bereich von virtuellen Administrationsservern kann von Organisationen mit komplexen Arbeitsabläufen verwendet werden.

Virtuelle Administrationsserver weisen die folgenden Einschränkungen auf:

- Virtuelle Administrationsserver werden ausschließlich im kommerziellen Modus von Kaspersky Next Expert View unterstützt.
- Für virtuelle Administrationsserver können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).
- Virtuelle Administrationsserver können nicht von Kaspersky Security Center nach Kaspersky Next Expert View migriert werden.
- Der für die Verwaltung des primären Administrationsservers zuständige Administrator verwaltet standardmäßig auch die virtuellen Administrationsserver.
- Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.
- Im Eigenschaftenfenster des virtuellen Administrationsservers ist die Anzahl der Abschnitte beschränkt.

Verteilungspunkt

Ein *Verteilungspunkt* 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.

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:

- Updates und Installationspakete an Client-Geräte innerhalb der Gruppe verteilen (einschließlich Verteilung mittels Multicast über das UDP-Protokoll). Updates können von Kaspersky-Update-Servern über eine Update-Aufgabe empfangen werden, die für den Verteilungspunkt erstellt wurde.

  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.

- Verteilen von Richtlinien und Gruppenaufgaben mittels Multicast über das UDP-Protokoll.
- Fungiert als Gateway für die Verbindung verwalteter Geräte zum Administrationsserver, da in der Cloud-Infrastruktur keine direkte Verbindung hergestellt werden kann.
- Abfragen des Netzwerks, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden.

- Remote-Installation von Drittanbieter-Programmen und Software von Kaspersky mittels Microsoft Windows-Tools und einschließlich der Installation auf Client-Geräten ohne installierten Administrationsagenten.

  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.

- Fungieren als Proxyserver, der an Kaspersky Security Network teilnimmt.

  Diese Funktion wird von Verteilungspunktgeräten unter Linux- oder macOS nicht unterstützt.

  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 ausgeführt.

Wenn Sie über 10.000 Geräte sowie mehrere virtuelle Server und Richtlinien einsetzen, wird es dringend empfohlen, Verteilungspunkte für die korrekte Funktion Ihrer Infrastruktur zu verwenden. Informationen zum Zuweisen eines Geräts als Verteilungspunkt finden Sie im Artikel Berechnung der Anzahl und Konfiguration der Verteilungspunkte.

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 installierten Administrationsagenten, müssen den Verteilungspunkten entsprechend der Administrationsgruppen manuell zugewiesen 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. Dabei darf sich das Gerät, das als Verteilungspunkt fungiert, nicht in der Administrationsgruppe befinden, welcher es zugewiesen wurde. 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 Netzwerkstandort kann nur für Geräte mit Windows-Betriebssystem bestimmt werden.

Kaspersky Next Expert View 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 Next Expert View einen Sicherheitsvorfall der Ereigniskategorie *Warnung*. Der Sicherheitsvorfall wird in den Eigenschaften des Geräts im Abschnitt **Sicherheitsvorfälle** 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.

Web-Plug-ins zur Verwaltung

Für die Remote-Verwaltung der Software von Kaspersky mithilfe von Kaspersky Next Expert View 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 Next Expert View und einer spezifischen Kaspersky-Anwendung. Mit einem Verwaltungs-Plug-in können Sie Aufgaben und Richtlinien für die Anwendung konfigurieren.

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 Next Expert View wird dabei für die Anzeige von Betriebsdaten und Ereignissen der Anwendung sowie für Statistiken, die von Client-Geräten weitergeleitet wurden, genutzt.

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 Next Expert View bietet eine 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, erlaubt Ihnen Kaspersky Next Expert View, *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.

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.

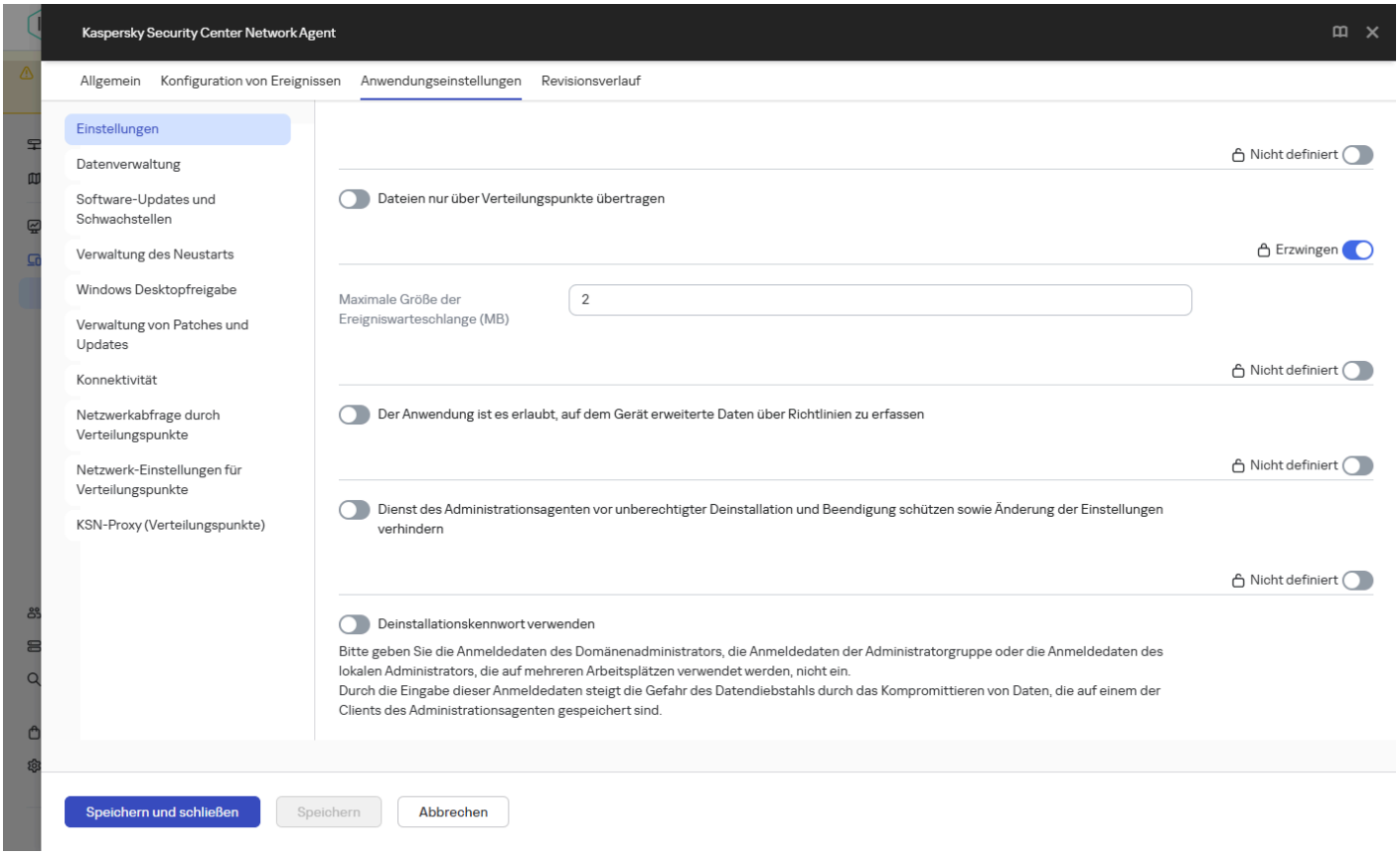
- Wenn die Änderung nicht unterbunden ist, verwendet die Anwendung den lokalen Einstellungswert auf jedem Client-Gerät und nicht den Wert, der in der Richtlinie angegeben ist. Der Einstellungswert kann dabei über die lokalen Anwendungseinstellungen geändert werden.

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.



Programmeinstellungen der Richtlinie

Lizenzierung des Programms

Dieser Abschnitt enthält Informationen zur Lizenzierung des Programms.

Lizenzierung von Kaspersky Next Expert View

Nach diesem Szenario können Sie die Kaspersky Next Expert View und verwaltete Sicherheitsanwendungen im Rahmen einer Lizenz verwenden.

Kaspersky Next Expert View ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Anwendungen auf Client-Geräte sowie die Überwachung der Schlüsselverwendung und die Verlängerung der Gültigkeitsdauer der Lizenz.

Wenn Sie die Kaspersky Next Expert View bereits verwenden, können Sie den Kaspersky Marketplace besuchen, um das gesamte Angebot an Kaspersky-Unternehmenslösungen anzuzeigen, die gewünschten Lösungen auszuwählen und mit dem Kauf auf der Kaspersky-Website fortfahren.

Ausprobieren der Funktionen von Kaspersky Next Expert View vor dem Erwerb einer Lizenz

Sie können die Kaspersky Next Expert View zunächst kostenlos testen. Erstellen Sie dazu einen Testarbeitsbereich, der nach 30 Tagen gelöscht wird. Wenn Sie einen kommerziellen Arbeitsbereich bevorzugen, den Sie so lange nutzen können, wie Sie möchten, müssen Sie eine Lizenz erwerben.

Schritte

Das Szenario verläuft in den folgenden Schritten:

1. **Abrufen eines Aktivierungscodes für die Lizenzierung der Kaspersky Next Expert View im kommerziellen Modus. Erwerb einer Lizenz (oder mehrerer Lizenzen)**

   Unterschiedliche Lizenzen ermöglichen die Nutzung verschiedener Anwendungen und Dienste von Kaspersky, sodass Sie möglicherweise mehrere Lizenzen erwerben möchten.

   Finden Sie heraus, welche Lizenzen Sie erwerben können und wie viele Geräte für jede Lizenz mindestens erforderlich sind.

   Die Kaspersky Next Expert View ist Bestandteil mehrerer Lösungen von Kaspersky. Wählen Sie aus, welche Lösung Sie verwenden möchten, und erwerben Sie eine Lizenz für diese. Wenn Sie eine Lizenz für 10.000 oder mehr Geräte erwerben möchten, müssen Sie sich mit einer speziellen Anfrage an Kaspersky oder einen der Partner von Kaspersky wenden.

   Verwenden Sie die Tabelle, um zu überprüfen, welche Funktionen des Schwachstellen- und Patch-Managements unter welcher Lizenz verfügbar sind.

   Wenn Sie die Kaspersky Next Expert View in einer Cloud-Umgebung wie Microsoft Azure verwenden möchten, lesen Sie mehr über die Optionen zur Lizenzierung für Cloud-Umgebungen.

Wenn Sie ein Managed Service Provider (MSP) sind, lesen Sie mehr über die Lizenzierung von Kaspersky Next Expert View für MSPs.

2. **Aktivierung der Kaspersky Next Expert View beim Erstellen des Arbeitsbereichs**

   Beim Erstellen eines Arbeitsbereichs geben Sie Ihren Lizenzschlüssel an, um Kaspersky Next Expert View zu aktivieren.

   Wenn Sie über mehrere Lizenzschlüssel verfügen, geben Sie einen davon an – später müssen Sie weitere Lizenzschlüssel in der Kaspersky Next Expert View hinzufügen, um verwaltete Kaspersky-Anwendungen zu aktivieren.

3. **Lizenzschlüssel für verwaltete Programme zur Datenverwaltung des Administrationsservers hinzufügen**

   Vor der Bereitstellung der Lizenzschlüssel müssen Sie diese Lizenzschlüssel der Datenverwaltung des Administrationsservers hinzufügen.

   Der Lizenzschlüssel, den Sie beim Erstellen des Arbeitsbereichs angegeben haben, wird der Datenverwaltung des Administrationsservers automatisch hinzugefügt.

   Wenn Sie mehr als einen Lizenzschlüssel haben, fügen Sie Ihre Lizenzschlüssel nacheinander der Datenverwaltung des Administrationsservers von Kaspersky Next Expert View hinzu.

4. **Lizenzschlüssel für verwaltete Programme bereitstellen**

   Wählen Sie eine Methode zur Bereitstellung des Lizenzschlüssels (oder der Lizenzschlüssel) auf allen Geräten, die Sie schützen möchten, aus:

   - Mittels automatischer Verteilung

     > Wenn Sie verschiedene verwaltete Programme verwenden und für Programme einen bestimmten Aktivierungscode bereitstellen möchten, wählen Sie eine andere Methode zur Verteilung des Aktivierungscodes.

     Kaspersky Security Center erlaubt für verwaltete Programme die automatische Verteilung von vorhandenen Lizenzschlüsseln. Angenommen, in der Datenverwaltung des Administrationsservers befinden sich drei Lizenzschlüssel. Sie haben die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** für alle drei Lizenzschlüssel aktiviert. Auf den Unternehmensgeräten ist eine Sicherheitsanwendung von Kaspersky installiert, z. B. Kaspersky Endpoint Security für Windows. Ein neues verwaltetes Programm wurde auf einem Gerät entdeckt und erfordert die Bereitstellung eines Lizenzschlüssels. In diesem Fall können beispielsweise zwei der Lizenzschlüssel aus der Datenverwaltung für das verwaltete Programm auf dem Gerät bereitgestellt werden: Lizenzschlüssel *Key_1* und Lizenzschlüssel *Key_2*. Einer dieser Lizenzschlüssel wird für das verwaltete Programm verteilt. In diesem Fall kann nicht vorausgesagt werden, welcher der beiden Lizenzschlüssel verteilt wird, da die automatische Verteilung von Lizenzschlüsseln keinerlei Aktivitäten des Administrators vorsieht.

     Bei der Verteilung des Lizenzschlüssels erfolgt eine erneute Zählung aller Installationen, für welche dieser Schlüssel gilt. Sie müssen sicherstellen, dass die Anzahl der Programme, für die der Lizenzschlüssel verteilt wird, die Lizenzbeschränkung nicht überschreitet. Falls die Anzahl der Installationen die Lizenzbeschränkung überschreitet, wird allen Geräten, die nicht durch die Lizenz abgedeckt sind, der Status *Kritisch* zugewiesen.

     Anleitung:

     - Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
     - Lizenzschlüssel automatisch verteilen

   - 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 anschließend die Geräte auf die von Ihnen bevorzugte Art auswählen, z. B. indem Sie eine Administrationsgruppe oder eine Geräteauswahl wählen.

Anleitung:

- 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.

5. **Feststellen, auf welchen Geräten die verwalteten Kaspersky-Anwendungen aktiviert sind**

   Um sicherzustellen, dass die Lizenzschlüssel korrekt bereitgestellt wurden, können Sie die Liste mit Lizenzschlüsseln anzeigen, die für ein Programm verwendet werden.

6. **Ereignisse im Zusammenhang mit dem Ablaufdatum der Lizenzen konfigurieren**

   Konfigurieren Sie Ereignisse, damit Sie benachrichtigt werden, wenn Ihre Lizenzschlüssel aufgebraucht sind oder demnächst ablaufen:

   - Ereignisse des Administrationsservers: Kritisch
   - Ereignisse des Administrationsservers: Funktionsfehler
   - Ereignisse des Administrationsservers: Warnung
   - Ereignisse des Administrationsservers: Information

Informationen über den Testmodus von Kaspersky Next Expert View

Der *Testmodus* ist ein spezieller Modus von Kaspersky Next Expert View, in dem sich der Benutzer mit den Funktionen von Kaspersky Next Expert View vertraut machen soll. Wenn Sie mit der Verwendung von Kaspersky Next Expert View beginnen, können Sie entweder einen Testarbeitsbereich anfordern oder einen Aktivierungscode für eine kommerzielle Lizenz eingeben. Wenn Sie einen Testarbeitsbereich anfordern, wird automatisch eine 30-tägige Demolizenz in den Arbeitsbereich eingebettet. Der im Testmodus verfügbare Funktionsumfang entspricht dem, der unter einer Lizenz für Kaspersky Next EDR Optimum bereitgestellt wird.

Wenn die Anwendung vor dem Ablaufdatum der Testversion mit einer kommerziellen Lizenz aktiviert wird, bleiben die Konfiguration des Arbeitsbereichs und alle zuvor hinzugefügten Geräte erhalten. Andernfalls wird nach Ablauf des Testzeitraums der Arbeitsbereich mit allen seinen Daten automatisch gelöscht.

Für die Verwendung der Funktionen von Expert View im Testmodus gelten folgende Einschränkungen:

- Sie können keine Administrationsserver-Hierarchie erstellen. Es können keine virtuellen Administrationsserver erstellt werden.
- Sie können keine benutzerdefinierten Installationspakete erstellen.
- Sie können keine benutzerdefinierten Rollen für Benutzer erstellen.
- Die Funktion für das Erkennen eines Virenangriffs ist nicht verfügbar. Ereignisse vom Typ "Virenangriff" werden nicht gespeichert und es werden keine Benachrichtigungen gesendet.

- Die Datenverwaltung für **gelöschte Objekte** ist nicht verfügbar.
- Das Hinzufügen von Massenereignissen (die in großen Mengen veröffentlicht wurden) zur Datenbank ist nicht möglich.
- Die Migration der Administrationsserver vom lokalen Modus in den Web Console-basierten Modus wird nicht unterstützt.
- Statistische KSN-Informationen von Komponenten des Administrationsservers, wie Administrationsserver oder Administrationsagent, werden nicht an Kaspersky gesendet.
- Die Integration mit den Active Directory Federation Services (AD FS) wird nicht unterstützt.
- Die Integration mit Microsoft Entra ID wird nicht unterstützt.

Auch für die Erstellung einiger Objekte des Programms gelten einige Beschränkungen (siehe Tabelle unten). Wird einer dieser Grenzwerte beim Versuch, ein solches Objekt zu erstellen, überschritten, wird der Vorgang blockiert und eine Fehlermeldung mit dem Grenzwert angezeigt.

Einschränkungen bei der Erstellung von Objekten in Expert View im Testmodus

Typ der Einschränkung	Wert
Richtlinien	30
Aufgaben	30
Lizenzschlüssel	5
Installationspakete	8
Geräteauswahlen (voreingestellte Instanzen nicht enthalten)	5
Ereignisauswahlen (voreingestellte Instanzen nicht enthalten)	5
Verschiebungsregeln für Geräte	3
Berichtsvorlagen desselben Typs	10
Interne Sicherheitsgruppen	20
Verwaltete Geräte	500

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 Next Expert View auf die entsprechende Produktseite innerhalb des Webauftritts von Kaspersky 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.

Lizenzen und die Mindestanzahl von Geräten für jede Lizenz

Wenn Sie Kaspersky Next Expert View im kommerziellen Modus verwenden möchten, müssen Sie eine Lizenz erwerben, bevor Sie Ihren ersten Arbeitsbereich anlegen können. Die untere Tabelle stellt die zur Verfügung stehenden Lizenzen und für jede Lizenz die Mindestanzahl an erforderlichen Geräten dar (selbst wenn Sie weniger Geräte schützen möchten):

Lizenzen, welche die Verwendung von Kaspersky Next Expert View erlauben

Lizenz	Minimale Anzahl an Geräten (selbst wenn Sie weniger Geräte schützen möchten)
Kaspersky Endpoint Security for Business Select	Für kommerzielle Lizenzen: 300 Für kommerzielle-Lizenzen (Abonnement): 100
Kaspersky Endpoint Security for Business Advanced	Für kommerzielle Lizenzen: 300 Für kommerzielle-Lizenzen (Abonnement): 100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	Für kommerzielle Lizenzen: 300 Für kommerzielle-Lizenzen (Abonnement): 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security, Desktop	Für kommerzielle Lizenzen: 300 Für kommerzielle-Lizenzen (Abonnement): 100
Kaspersky Hybrid Cloud Security, Server	50
Kaspersky Hybrid Cloud Security, Core	20
Kaspersky Hybrid Cloud Security, CPU	20
Kaspersky Hybrid Cloud Security Enterprise, Desktop	Für kommerzielle Lizenzen: 300 Für kommerzielle-Lizenzen (Abonnement): 100
Kaspersky Hybrid Cloud Security Enterprise, Server	50
Kaspersky Hybrid Cloud Security Enterprise, CPU	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphonie (derzeit nur in Russland verfügbar)	300
Kaspersky Next EDR Foundations	Für kommerzielle Lizenzen: 300 Benutzer Für kommerzielle-Lizenzen (Abonnement): 100 Benutzer Jede Benutzerlizenz deckt 1 PC-/Mac-Gerät und 2 mobile Geräte ab.
Kaspersky Next EDR Optimum	Für kommerzielle Lizenzen: 300 Benutzer Für kommerzielle-Lizenzen (Abonnement): 100 Benutzer Jede Benutzerlizenz deckt 1 PC-/Mac-Gerät und 2 mobile Geräte ab.
Kaspersky Next Complete Security	Für kommerzielle Lizenzen: 300 Benutzer Für kommerzielle-Lizenzen (Abonnement): 100 Benutzer Jede Benutzerlizenz deckt 1 PC-/Mac-Gerät und 2 mobile Geräte ab.
Kaspersky Next EDR Expert	250 Benutzer Jede Benutzerlizenz deckt 1 PC-/Mac-Gerät und 2 mobile Geräte ab.
Kaspersky Next XDR Expert	250 Benutzer Jede Benutzerlizenz deckt 1 PC-/Mac-Gerät und 2 mobile Geräte ab.
Kaspersky Next MXDR Optimum	300 Benutzer

Lizenz	Minimale Anzahl an Geräten (selbst wenn Sie weniger Geräte schützen möchten)
Kaspersky XDR Optimum (derzeit nur in Russland und der GUS verfügbar)	Für kommerzielle Lizenzen: 300 Benutzer Für kommerzielle-Lizenzen (Abonnement): 100 Benutzer
Kaspersky Next XDR Optimum	Für kommerzielle Lizenzen: 300 Benutzer Für kommerzielle-Lizenzen (Abonnement): 100 Benutzer Jede Benutzerlizenz deckt 1 PC-/Mac-Gerät und 2 mobile Geräte ab.

Wenn Sie mehr als 10.000 Geräte schützen möchten, senden Sie bitte eine Anfrage an den Technischen Support von Kaspersky und geben Sie Informationen zu dem Arbeitsbereich an, den Sie erstellen möchten.

Ereignisse bei Überschreitung der Lizenzbeschränkung

Kaspersky Next Expert View ermöglicht das automatische Empfangen von Informationen über Ereignisse bei 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.

Methoden zur Verteilung von Aktivierungscodes an verwaltete Geräte

Jede der auf den verwalteten Geräten installierten Kaspersky-Anwendungen muss entweder mit einer Schlüsseldatei, mit einem Lizenzschlüssel oder mit einem Aktivierungscode lizenziert werden. Sie können keine Schlüsseldateien zur Lizenzierung verwalteter Programme verwenden. Es werden nur Aktivierungscodes akzeptiert. Ein Aktivierungscode kann folgendermaßen bereitgestellt werden:

- Mittels automatischer Verteilung
- Mittels der Aufgabe "Lizenzschlüssel hinzufügen" für ein verwaltetes Programm
- Mittels manueller Aktivierung eines verwalteten Programms

Kaspersky-Anwendungen können mehrere Lizenzschlüssel gleichzeitig verwenden. Kaspersky Endpoint Security für Windows kann beispielsweise zwei Lizenzschlüssel verwenden – einen für Kaspersky Endpoint Security für Windows und einen für die Aktivierung der integrierten Funktionen von Endpoint Detection and Response.

Darüber hinaus können Kaspersky-Anwendungen nicht nur über einen aktiven Lizenzschlüssel, sondern auch über einen Reserve-Lizenzschlüssel verfügen. Kaspersky-Anwendungen verwenden zum aktuellen Zeitpunkt einen aktiven Schlüssel und speichern einen Reserveschlüssel, der nach Ablauf des aktiven Schlüssels angewendet wird. Sie können mit einer der oben aufgeführten Methoden einen neuen aktiven Lizenzschlüssel oder einen Reserve-Lizenzschlüssel hinzufügen. Das Programm, für welches 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.

Lizenzschlüssel des Administrationsservers hinzufügen

Um einen Lizenzschlüssel des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wechseln Sie zum Abschnitt **Lizenzschlüssel** und klicken Sie anschließend in einem der folgenden Abschnitte auf die Schaltfläche **Auswählen**:

   - **Aktuelle Lizenz**, wenn Sie einen aktiven Lizenzschlüssel hinzufügen möchten.
   - **Reserve-Lizenzschlüssel**, wenn Sie einen Reserve-Lizenzschlüssel hinzufügen möchten.

     Sie können einen Reserve-Lizenzschlüssel nur hinzufügen, wenn bereits ein aktiver Lizenzschlüssel hinzugefügt wurde.

3. Wählen Sie neuen Fenster den gewünschten Lizenzschlüssel aus der Tabelle aus.

   Bei Bedarf können Sie einen neuen Lizenzschlüssel hinzufügen, indem Sie auf die Schaltfläche **Neuen Lizenzschlüssel hinzufügen** klicken und den Lizenzschlüssel anschließend im neuen rechten Fensterbereich eingeben.

4. Klicken Sie auf die Schaltfläche **OK**.

Das Fenster wird geschlossen, der Lizenzschlüssel für den Administrationsserver wird hinzugefügt und die Informationen über den Lizenzschlüssel werden im Abschnitt **Lizenzschlüssel** angezeigt.

Bei Bedarf können Sie den ausgewählten Lizenzschlüssel ändern, indem Sie auf die Schaltfläche **Ändern** klicken und einen anderen Lizenzschlüssel angeben. Sie können außerdem einen Lizenzschlüssel entfernen.

Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen

Beim Hinzufügen eines Lizenzschlüssels über Kaspersky Next Expert View werden die Lizenzschlüssel-Einstellungen auf dem Administrationsserver gespeichert. Anhand dieser Informationen erstellt das Programm 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.

Um einen Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. 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 auf Client-Geräte verteilen

Die Kaspersky Next Expert View ermöglicht die Verteilung von Lizenzschlüsseln auf Client-Geräte entweder mittels automatischer Verteilung oder mittels der Aufgabe **Anwendungsaktivierung**. 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 **Anwendungsaktivierung**, 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 **Anwendungsaktivierung**:*

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **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 **Anwendung** die Anwendung aus, für das Sie einen Lizenzschlüssel hinzufügen möchten.
4. Wählen Sie in der Liste **Aufgabentyp** die Aufgabe **Anwendungsaktivierung** 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 **Anwendungsaktivierung** 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 Next Expert View 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. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzen**.
2. Klicken Sie auf den Namen des Lizenzschlüssels, den Sie automatisch auf die Geräte verteilen möchten.
3. Setzen Sie im nächsten Fenster mit den Eigenschaften des Lizenzschlüssels den Schalter auf **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 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.

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.

Wenn Sie für einen Abonnement-Lizenzschlüssel die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** zum Aktivieren einer beliebigen Anwendung auf einem verwalteten Gerät angeben, und Sie gleichzeitig über einen aktiven Demolizenz-Schlüssel verfügen, wird Ihr Demolizenz-Schlüssel acht Tage vor dem Ablaufdatum automatisch durch den Abonnement-Lizenzschlüssel ersetzt.

Informationen zu den verwendeten Lizenzschlüsseln in der Datenverwaltung des Administrationsservers anzeigen

Um eine Liste der Lizenzschlüssel anzuzeigen, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzen**.

Die angezeigte Liste enthält die 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** → **Lizenzen**.
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
- Auf der Registerkarte **Beschränkungen**: die Liste der Lizenzbeschränkungen

  Wenn Sie den Administrationsserver unter einer Lizenz von Kaspersky Next XDR Optimum aktiviert haben, wird auf der Registerkarte **Beschränkungen** das Feld **XDR-O** mit dem Wert **Enabled** angezeigt.

Informationen zu den Lizenzschlüsseln für ein bestimmtes Kaspersky-Programm anzeigen

Um zu erfahren, welche Lizenzschlüssel von einer Kaspersky-Anwendung verwendet werden, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.

   Wenn das Gerät zur Gruppe nicht zugeordneter Geräte gehört, wechseln Sie stattdessen zu **Gerätesuche und Bereitstellung → Nicht zugeordnete Geräte**.

2. Klicken Sie auf den Namen des gewünschten Geräts.

3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts den Abschnitt **Anwendungen** aus.

4. Wählen Sie in der sich öffnenden Programmliste das Programm aus, dessen Lizenzschlüssel Sie anzeigen möchten.

5. Wählen Sie im sich öffnenden Fenster mit den Programmeigenschaften auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel**.

   Die Informationen werden im Arbeitsbereich dieses Abschnitts angezeigt.

Lizenzschlüssel des Administrationsservers entfernen

Um einen Lizenzschlüssel des Administrationsservers zu entfernen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

2. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers den Abschnitt **Lizenzschlüssel** aus.

3. Klicken Sie je nachdem, welchen Lizenzschlüssel Sie entfernen möchten, auf die Schaltfläche **Aktiven Lizenzschlüssel entfernen** oder **Reserve-Lizenzschlüssel entfernen**, und bestätigen Sie anschließend den Vorgang im neuen Fenster.

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 aus der Datenverwaltung entfernen

Sie können einen Lizenzschlüssel aus der Datenverwaltung des Administrationsservers entfernen. Beachten Sie, dass Kaspersky Next Expert View in folgenden Fällen Ihren Arbeitsbereich automatisch nach 90 Tagen löscht:

- Sie entfernen den letzten, manuell zur Datenverwaltung hinzugefügten, Lizenzschlüssel (aktiv, als Reserve oder nicht verwendet).
- Der letzte Lizenzschlüssel läuft ab.

Wenn Ihr Arbeitsbereich gelöscht ist, können Sie den Schutz Ihres Netzwerks nicht mehr mit Kaspersky Next Expert View verwalten. Außerdem verlieren Sie unwiderruflich alle Daten von Kaspersky Next Expert View. Bei Bedarf können Sie Ihren Arbeitsbereich manuell löschen. Andernfalls empfehlen wir, mindestens einen Lizenzschlüssel in der Datenverwaltung des Administrationsservers aufzubewahren.

Wenn Sie einen Lizenzschlüssel entfernen, und bereits einen Reserve-Lizenzschlüssel hinzugefügt haben, wird der Reserve-Lizenzschlüssel automatisch zum aktiven Lizenzschlüssel, nachdem der frühere Lizenzschlüssel entfernt wurde oder abgelaufen ist.

Wenn Sie den aktiven Lizenzschlüssel entfernen, der auf einem verwalteten Gerät bereitgestellt wurde, bleibt das Programm auf dem verwalteten Gerät weiterhin funktionsfähig.

So entfernen Sie einen Lizenzschlüssel aus der Datenverwaltung des Administrationsservers:

1. Prüfen Sie, dass der von Ihnen zu entfernende Lizenzschlüssel nicht vom Administrationsserver verwendet wird. Ein Schlüssel, der vom Administrationsserver verwendet wird, kann nicht entfernt werden. So können Sie dies prüfen:

   a. Öffnen Sie das Eigenschaftsfenster des Administrationsservers:

      a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

      b. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen des erforderlichen Administrationsservers und klicken Sie anschließend auf das Einstellungssymbol (⚙).

   Alternativ können Sie auf den Namen des Administrationsservers klicken und wenn der Name anschließend im Hauptmenü angezeigt wird, auf diesen klicken, um das Eigenschaftsfenster des Servers zu öffnen.

   b. Wählen Sie im neuen Fenster mit den Eigenschaften des Administrationsservers auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel**.

   c. Wenn der erforderliche Lizenzschlüssel 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 der erforderliche Lizenzschlüssel nicht angezeigt, so wird er vom Administrationsserver nicht verwendet.

2. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzen**.

3. Wählen Sie den erforderlichen Lizenzschlüssel aus und klicken Sie auf die Schaltfläche **Löschen**.

4. Aktivieren Sie im neuen Fenstern das Kontrollkästchen **Ich kenne das Risiko und möchte den Lizenzschlüssel entfernen**. Dies bedeutet, dass Sie sich darüber im Klaren sind, dass nach dem Entfernen des letzten Lizenzschlüssels ebenso der Arbeitsbereich gelöscht wird und die Kontrolle über die verwalteten Geräte verloren geht. Klicken Sie anschließend auf die Schaltfläche **Entfernen**.

Infolgedessen wird der ausgewählte Lizenzschlüssel aus der Datenverwaltung entfernt.

Sie können einen entfernten Lizenzschlüssel erneut hinzufügen oder einen neuen Schlüssel hinzufügen. Wenn Sie den letzten Lizenzschlüssel entfernt haben, können Sie ebenfalls einen Lizenzschlüssel hinzufügen, solange der Arbeitsbereich noch nicht gelöscht wurde. Kaspersky Next Expert View benachrichtigt die Administratoren des Arbeitsbereichs 30 Tage, 7 Tage und 1 Tag vor der Löschung.

Liste mit Geräten anzeigen, auf denen sich ein nicht aktiviertes Kaspersky-Programm befindet

Sie können die Liste aller Geräte anzeigen, auf denen eine Kaspersky-Anwendung installiert, aber nicht aktiviert ist (z. B. aufgrund einer fehlenden oder abgelaufenen Lizenz).

So zeigen Sie die Geräte an, auf denen sich eine nicht aktivierte Kaspersky-Anwendung befindet:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Aufgaben**.

   Die Aufgabenliste wird angezeigt.

2. Klicken Sie auf den Namen der Updateaufgabe für die betreffende Kaspersky-Anwendung.

   Das Fenster mit den Aufgabeneigenschaften enthält mehrere benannte Registerkarten.

3. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Ergebnisse** aus.

   In der Spalte **Gerät oder sekundärer Server** werden die Geräte angezeigt, auf denen die Aufgabe erfolgreich war.

4. Sortieren Sie die Spalte **Gerät oder sekundärer Server**.

   In der Spalte **Gerät oder sekundärer Server** werden die Geräte angezeigt, auf denen die Aufgabe erfolgreich war. Die Geräte, auf denen die Aufgabe aufgrund einer fehlenden Lizenz fehlgeschlagen ist, sind die Geräte, auf denen das Programm nicht aktiviert ist.

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 und seine Installationspakete deinstallieren. Die Installationspakete müssen vom Administrationsserver und seinen virtuellen Administrationsservern gelöscht werden.

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. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** im Eigenschaftenfenster des Administrationsservers den Abschnitt **Endbenutzer-Lizenzverträge** aus.

   Es wird eine Liste von EULAs angezeigt, die beim Erstellen von Installationspaketen oder bei der nahtlosen Installation von Updates akzeptiert wurden.

3. 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.
   - Ob die EULA widerrufen werden kann oder nicht.

4. 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) und ihrer entsprechenden Namen und Typen.

5. Klicken Sie im unteren Teil des EULA-Eigenschaftenfensters auf die Schaltfläche **Lizenzvertrag widerrufen**.

   Wenn die ausgewählte EULA nur durch die Deinstallation des Programms oder nur auf dem primären Administrationsserver widerrufen werden kann, wird anstelle der Schaltfläche **Lizenzvertrag widerrufen** eine Nachricht über diese Einschränkung angezeigt.

   Sollten Objekte (Installationspakete und ihre entsprechenden Aufgaben) existieren, die den Widerruf der EULA verhindern, wird eine Nachricht darüber 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.

6. 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.

Wenn der letzte Lizenzschlüssel abgelaufen ist, löscht Kaspersky Next Expert View Ihren Arbeitsbereich automatisch nach 90 Tagen. Infolgedessen können Sie den Schutz Ihres Netzwerks nicht mehr mit Kaspersky Next Expert View verwalten. Außerdem verlieren Sie unwiderruflich alle Daten von Kaspersky Next Expert View. Um Ihren Arbeitsbereich zu behalten, empfehlen wir, eine abgelaufene Lizenz zu verlängern oder zur Datenverwaltung des Administrationsservers eine neue Lizenz hinzuzufügen.

So zeigen Sie Benachrichtigungen über Lizenzen an, die entweder abgelaufen oder kurz vor dem Ablaufen sind:

1. Führen Sie eine beliebige der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzen**.
   - Wechseln Sie im Hauptmenü zu **Überwachung** → **Dashboard** und klicken Sie anschließend auf den Link **Ablaufende Lizenzen anzeigen** neben einer Benachrichtigung.

   Es öffnet sich das Fenster **Lizenzen**, in dem Sie ablaufende und abgelaufene Lizenzen anzeigen und erneuern können.

2. Wenn Sie eine Lizenz verlängern möchten, klicken Sie neben der erforderlichen Lizenz auf den Link **Lizenz verlängern**.

   Durch Klicken auf einen Link zur Lizenzverlängerung erklären Sie sich damit einverstanden, die folgenden Daten an Kaspersky zu übertragen: Software-ID, Softwareversion, Softwarelokalisierung, Lizenz-ID und ein Attribut, das angibt, ob die Lizenz von einem Partnerunternehmen bereitgestellt wurde. Diese Daten werden benötigt, um die Bedingungen für die Verlängerung Ihrer Lizenz zu bestimmen.

3. Folgen Sie im sich öffnenden Fensters des Dienstes für Lizenzverlängerung den Anweisungen um eine Lizenz zu verlängern.

   Die ablaufende Lizenz wird verlängert.

In der Kaspersky Next Expert View 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 Next Expert View nach Ablauf der Lizenz verwenden

Nach Ablauf der Lizenz kann Ihnen Kaspersky die weitere uneingeschränkte Nutzung der Kaspersky Next Expert View für bis zu 90 Tage gewähren. Während dieses Zeitraums werden der Administrationsserver, der Administrationsagent und die Web-Oberfläche von Kaspersky Next Expert View ohne Einschränkungen ausgeführt. Kaspersky Next Expert View übermittelt außerdem entsprechen den aktuellen KSN-Einstellungen die KSN-Statistiken an Kaspersky. Die verwalteten Programme werden nur mit eingeschränkter Funktionalität ausgeführt (Weitere Informationen dazu finden Sie in den Dokumentationen dieser Anwendungen).

90 Tage nach Ablauf der Gültigkeit der Lizenz löscht Kaspersky Next Expert View Ihren Arbeitsbereich automatisch. Wenn Sie den Arbeitsbereich behalten möchten, müssen Sie mindestens einen abgelaufenen Lizenzschlüssel verlängern oder einen neuen Lizenzschlüssel zur Datenverwaltung hinzufügen.

Lizenzdefinitionen

Dieser Abschnitt enthält Definitionen von Konzepten zur Lizenzierung von Kaspersky-Anwendungen, die mittels Kaspersky Next Expert View verwaltet werden.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für Kaspersky Next Expert View, 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 der Testlizenz abgelaufen ist, stellt Kaspersky Next Expert View 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 Programmfunktionen deaktiviert. Zur weiteren Nutzung von Kaspersky Next Expert View ist eine Verlängerung der kommerziellen Lizenz erforderlich. Nach Ablauf einer kommerziellen Lizenz können Sie das Programm 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 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 dem Programm einen Lizenzschlüssel hinzufügen, indem Sie einen *Aktivierungscode* eingeben. Nachdem Sie den Lizenzschlüssel im Programm hinzugefügt haben, wird er auf 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 den Aktivierungscode

Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus 20 Buchstaben und Ziffern. Sie geben einen Aktivierungscode ein, um einen Lizenzschlüssel hinzuzufügen, der die Kaspersky Next Expert View aktiviert. Sie erhalten den Aktivierungscode an die von Ihnen angegebene E-Mail-Adresse, nachdem Sie Kaspersky Next Expert View erworben haben oder eine Testversion von Kaspersky Next Expert View angefordert 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 die Anwendung 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.

Über das Abonnement

Ein *Abonnement für Kaspersky Next Expert View* ist eine Bestellung des Programms mit bestimmten Einstellungen (Ablaufdatum des Abonnements, Anzahl der geschützten Geräte). Ein Abonnement für Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View 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 Next Expert View 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 Next Expert View verwendet werden.

Bei einer Nutzung des Programms im Abonnement stellt Kaspersky Next Expert View zum festgelegten Zeitpunkt vor Ablauf des Abonnements automatisch eine Verbindung zum Aktivierungsserver her. 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.

Bereitstellung von Daten

Mit der Kaspersky Next Expert View kann der Benutzer die Geräte (und die Gerätebesitzer), die mit der Kaspersky Next Expert View verbunden sind, mittels der Funktionen der verwalteten Programme identifizieren und steuern.

Methoden zur Bereitstellung von Daten:

1. Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Next Expert View ein.
2. Der Administrationsagent erhält Daten von dem Gerät und übermittelt sie an den Administrationsserver.
3. Der Administrationsagent empfängt von dem durch Kaspersky verwalteten Programm abgerufenen Daten und überträgt sie an den Administrationsserver. Die Liste der Daten, die durch Programme verarbeitet werden, welche von Kaspersky verwaltet werden, finden Sie in der Hilfe der entsprechenden Programme.
4. Die Daten werden von lokal ausgeführten sekundären Administrationsservern übertragen.

Kaspersky Next Expert View löscht Arbeitsbereiche automatisch 30 Tage nach Ablauf der Gültigkeitsdauer der Testlizenz und 90 Tage nach Ablauf der kommerziellen Lizenz.

Nach Ablauf der Gültigkeitsdauer der Lizenz speichert Kaspersky die Benutzerdaten in Bezug auf Alarme und Vorfälle für 30 Tage in den Arbeitsbereichen des Benutzers.

Unter der aktuellen Lizenz beträgt die Speicherdauer für Alarme und Vorfälle 360 Tage. Nach diesem Zeitraum werden ältere Alarme und Vorfälle automatisch gelöscht.

Die endgültige Löschung der in diesem Abschnitt aufgeführten Daten kann bis zu 24 Stunden dauern.

An Kaspersky-Server gesendete Daten

Daten, die im Rahmen der Aktivierung gesendet werden

Bei Verwendung des Aktivierungscodes zur Aktivierung der Software erklärt der Benutzer sein Einverständnis damit, Kaspersky regelmäßig die folgenden Informationen zur Verfügung zu stellen, um die Rechtmäßigkeit der Verwendung der Software zu überprüfen:

- Aktivierungscode
- Eindeutige Aktivierungskennung der aktuellen Lizenz

Kaspersky kann diese Informationen auch verwenden, um statistische Informationen über die Verteilung und Verwendung der Software von Kaspersky zu generieren.

Daten, die im Rahmen der Aktualisierung gesendet werden

Nach Erhalt von Updates von den Update-Servern des Rechteinhabers verpflichtet sich der Benutzer, Kaspersky regelmäßig die folgenden Informationen zur Verfügung zu stellen, um die Qualität des Update-Mechanismus zu verbessern:

- Die von der Lizenz bezogene Software-ID
- Die vollständige Version der Software
- Die Software-Lizenz-ID
- Die Software-Installations-ID (PCID)
- Die Start-ID des Programm-Updates

Kaspersky kann diese Informationen auch verwenden, um statistische Informationen über die Verteilung und Verwendung der Software von Kaspersky zu generieren.

Daten zur Gewährleistung eines unterbrechungsfreien Betriebs sowie einer effizienten Ausführung und zur Überprüfung der rechtmäßigen Verwendung von Kaspersky Next Expert View

Die folgenden Informationen können für den angegebenen Zweck verwendet werden:

- Namen und Versionen der mit dem Arbeitsbereich verbundenen Kaspersky-Sicherheitsanwendungen sowie die Anzahl der Geräte, auf denen diese Sicherheitsanwendungen installiert sind.
- Anzahl der Geräte mit installierten Kaspersky-Sicherheitsanwendungen, die mit allen Arbeitsbereichen verbunden wurden, und Verteilung dieser verbundenen Geräte nach deren Typen.
- Arbeitsbereichs-ID, Land und Region des Arbeitsbereichs und Erstellungsdatum des Arbeitsbereichs.
- Anzahl der Benutzer im Arbeitsbereich, Datum der letzten Authentifizierung im Arbeitsbereich.
- Details zu der aktuell verwendeten Lizenz, Lizenztyp, Lizenzbeschränkung in Bezug auf die Anzahl der Geräte, Anzahl der verbundenen Geräte und Ablaufdatum der zuvor verwendeten Lizenz.

Daten, die beim Folgen der Links in der Benutzeroberfläche von Kaspersky Next Expert View übertragen werden

Durch folgen der Links in der Verwaltungskonsole oder der Kaspersky Next Expert View stimmt der Nutzer zu, die folgenden Daten automatisch zu übertragen:

- Lokalisierung von Kaspersky Next Expert View
- Lizenz-ID
- 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.

Daten für den Betrieb von verwalteten Programmen

Die folgenden verwalteten Programme übertragen die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver:

- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security für Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Endpoint Security für Android
- Kaspersky Security für iOS
- Kaspersky Secure Mobility Management
- Kaspersky Embedded Systems Security für Windows
- Kaspersky Embedded Systems Security für Linux

Die Liste der verarbeiteten Daten ist in der Vereinbarung über die von Kaspersky Next verarbeiteten Daten beim Verbinden eines Geräts beschrieben.

Lokal verarbeitete Daten

Die einzige Komponente von Kaspersky Security Center, die lokal in einer Kaspersky Next Expert View bereitgestellt werden kann, ist der Administrationsagent.

Liste von lokal verarbeiteten Benutzerdaten:

- Alle im Abschnitt "Benutzerdaten" aufgeführten Daten, die im Rahmen der Ausführung und in der Infrastruktur von Kaspersky verarbeitet werden. Ausnahmen sind die Daten, die der Administrator über die Benutzeroberfläche von Kaspersky Next Expert View eingibt
- Kaspersky-Ereignisprotokoll des Administrationsagenten
- Ablaufverfolgung des Administrationsagenten
- Protokolle, einschließlich der vom Installationsprogramm des Administrationsagenten und den Dienstprogrammen von Kaspersky Security Center erstellten Protokolle

Die Dump-, Log- und Protokolldateien des Administrationsagenten enthalten zufällige Daten und möglicherweise personenbezogene Daten. Die Dateien werden unverschlüsselt auf dem Gerät gespeichert, auf dem der Administrationsagent installiert ist. Die Dateien werden nicht automatisch an Kaspersky übertragen. Der Benutzer kann diese Daten auf Anfrage des technischen Supports manuell an Kaspersky übertragen, um Probleme beim Betrieb von Kaspersky Security Center zu beheben.

Über die rechtlichen Dokumente für Kaspersky Next Expert View

Um Kaspersky Next Expert View verwenden zu können, müssen Sie Ihre Zustimmung zu den Bestimmungen und Bedingungen der auf der Website von Kaspersky Next Expert View angegebenen rechtlichen Dokumente geben. Sie können die Bestimmungen und Bedingungen der Datenschutzrichtlinie von AO Kaspersky Lab für Websites anzeigen, wenn Sie sich bei der Kaspersky Next Expert View anmelden, um einen Arbeitsbereich zu verwalten. Sie können die Vereinbarung der Kaspersky Next Expert View und die Vereinbarung zur Datenverarbeitung von Kaspersky Next Expert View lesen, wenn Sie einen Unternehmensarbeitsbereich erstellen.

Bitte lesen Sie sich die Texte aller rechtlichen Dokumente sorgfältig durch, bevor Sie mit der Verwendung von Kaspersky Next Expert View beginnen.

Endbenutzer-Lizenzvertrag für Kaspersky-Anwendungen

Der Endbenutzer-Lizenzvertrag (im weiteren Text entweder Lizenzvertrag oder EULA genannt) ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab, der festlegt, zu welchen Bedingungen Sie die Kaspersky-Anwendungen nutzen dürfen.

Sie haben die folgenden Möglichkeiten, um sich mit den Bedingungen des Endbenutzer-Lizenzvertrags vertraut zu machen:

- Im Fenster, das beim Erstellen eines Installationspakets für eine Kaspersky-Anwendung angezeigt wird.
- In der Datei license.txt, im Installationsordner der Kaspersky-Anwendung, auf dem verwalteten Gerät.

Sie können jederzeit Ihre Akzeptanz des Endbenutzer-Lizenzvertrags widerrufen.

Wenn Sie den Endbenutzer-Lizenzvertrag einer Kaspersky-Anwendung nicht akzeptieren, können Sie diese Anwendung nicht verwenden.

Härtungsleitfaden

Kaspersky Next Expert View ist ein Programm, das von Kaspersky gehostet und verwaltet wird. Sie müssen Kaspersky Next Expert View nicht auf Ihrem Computer oder Server installieren. Mit Kaspersky Next Expert View kann der Administrator Kaspersky-Sicherheitsanwendungen auf Geräten in einem Unternehmensnetzwerk installieren, Untersuchungs- und Updateaufgaben remote ausführen und die Sicherheitsrichtlinien verwalteter Anwendungen verwalten.

Kaspersky Next Expert View 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 Next Expert View können Sie alle Schutzkomponenten konfigurieren, die mithilfe von Kaspersky-Anwendungen erstellt wurden.

Die Kaspersky Next Expert View hat vollen Zugriff auf die Schutzverwaltung der Client-Geräte und ist die wichtigste Komponente des Sicherheitssystems der Organisation. Daher sind für Kaspersky Next Expert View erhöhte Schutzmaßnahmen erforderlich.

Der Härtungsleitfaden enthält Empfehlungen und Funktionen zur Konfiguration von Kaspersky Next Expert View und ihren Komponenten, mit dem Ziel, das Risiko einer Kompromittierung zu verringern.

Der Härtungsleitfaden enthält die folgenden Informationen:

- Konfiguration der Benutzerkonten in Kaspersky Next Expert View
- Verwaltung des Schutzes der Client-Geräte
- Konfigurieren des Schutzes für verwaltete Programme
- Übertragen von Informationen an Programme von Drittanbietern

Bevor Sie mit der Verwendung von Kaspersky Next Expert View beginnen, werden Sie dazu aufgefordert, die Kurzversion des Härtungsleitfadens zu lesen.

Beachten Sie, dass Sie Kaspersky Next Expert View erst verwenden können, nachdem Sie bestätigt haben, dass Sie den Härtungsleitfaden gelesen haben.

So können Sie den Härtungsleitfaden lesen:

1. Öffnen Sie die Kaspersky Next Expert View und melden Sie sich an. Kaspersky Next Expert View prüft, ob Sie das Lesen der aktuellen Version des Härtungsleitfadens bestätigt haben.

   Wenn Sie den Härtungsleitfaden noch nicht gelesen haben, öffnet sich ein Fenster und zeigt eine Kurzfassung von ihm 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 die Kaspersky Next Expert View jetzt verwenden.

Wenn eine neue Version des Härtungsleitfadens veröffentlicht wird, werden Sie von Kaspersky Next Expert View dazu aufgefordert, diese zu lesen.

Die Architektur von Kaspersky Next Expert View planen

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 des Architekturentwurfs empfehlen wir, sich mit den Komponenten von Kaspersky Next Expert View und ihren Wechselwirkungen untereinander, sowie mit den Schemata für Datenverkehr und Portnutzung vertraut zu machen.

Basierend auf diesen Informationen können Sie eine Architektur entwerfen, in der folgendes berücksichtigt wird:

- Organisation der Administrator-Arbeitsbereiche und Methoden zur Verbindung mit der Kaspersky Next Expert View
- 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

Konten und Authentifizierung

Verwendung der zweistufigen Überprüfung in der Kaspersky Next Expert View

Kaspersky Security Center Cloud Console bietet eine zweistufige Überprüfung für Benutzer.

Die zweistufige Überprüfung kann Ihnen dabei helfen, die Sicherheit Ihres Benutzerkontos in der Kaspersky Next Expert View zu erhöhen. Wenn diese Funktion aktiviert ist, müssen Sie bei jeder Anmeldung bei Kaspersky Next Expert View mit Ihrer E-Mail-Adresse und Ihrem Kennwort zusätzlich einen Einmal-Sicherheitscode eingeben. Sie können einen einmaligen Sicherheitscode entweder per SMS erhalten oder in Ihrer Authenticator-App generieren (gemäß der von Ihnen eingerichteten Methode zur zweistufigen Überprüfung).

Es wird dringend davon abgeraten, die Authenticator-App auf demselben Gerät zu installieren, von dem aus die Verbindung zur Kaspersky Next Expert View hergestellt wird. Sie können eine Authenticator-App auf Ihrem Mobilgerät installieren.

Verbieten der Speicherung des Administratorpassworts

Wenn Sie Kaspersky Next Expert View verwenden, **raten wir dringend davon ab**, das Administratorkennwort in einem auf dem Benutzergerät installierten Browser zu speichern.

Bei einer Kompromittierung des Browsers kann ein Eindringling Zugriff auf die gespeicherten Kennwörter erhalten. Auch bei Diebstahl oder Verlust eines Benutzergeräts mit darauf gespeicherten Kennwörtern kann sich ein Eindringling Zugriff auf geschützte Daten verschaffen.

Einschränken der Rolle "Hauptadministrator"

Wir empfehlen, für die Rolle Hauptadministrator die Zugehörigkeiten einzuschränken.

Nachdem ein Benutzer einen Arbeitsbereich erstellt hat, wird diesem Benutzer standardmäßig die Rolle "Hauptadministrator" zugewiesen. Sie ist sinnvoll für die 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.

Sie können die vordefinierten Benutzerrollen mit einem vorkonfigurierten Satz an Rechten für die Administration der Kaspersky Next Expert View verwenden.

Zugriffsrechte auf Programmfunktionen konfigurieren

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

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 Berechtigungen oder eine Rolle zuweisen.

Verwaltung des Schutzes der Client-Geräte

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.
- Als KSN-Proxyserver für Client-Geräte fungieren.

Unter Berücksichtigung der verfügbaren Funktionen empfehlen wir, alle Geräte, die als Verteilungspunkte fungieren, vor jeglicher Art von unbefugtem Zugriff (einschließlich physischem) zu schützen.

Konfigurieren des Schutzes für verwaltete Programme

Netzwerkschutz konfigurieren

Stellen Sie sicher, dass Sie das Szenario der Erstkonfiguration von Kaspersky Next Expert View abgeschlossen haben. Dieses Szenario umfasst auch die Ausführung der Schritte des Schnellstartassistenten.

Wenn der Schnellstartassistent ausgeführt wird, werden Richtlinien und Aufgaben mit Standardparametern erstellt. Diese Parameter sind möglicherweise nicht optimal oder in Ihrer Organisation möglicherweise sogar verboten. Daher empfehlen wir die Konfiguration der erstellten Richtlinien und Aufgaben und das bei Bedarf zusätzliche Erstellen von Richtlinien und Aufgaben für das Netzwerk Ihrer Organisation.

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 beispielsweise ein Kennwort für Kaspersky Endpoint Security für Windows, den Administrationsagenten und weitere Kaspersky-Anwendungen festlegen. Nachdem Sie den Kennwortschutz aktiviert haben, wird es empfohlen, diese Einstellungen zu sperren, indem Sie das "Schloss" schließen.

Angeben des Kennworts für das Tool "klmover" und Entfernen des Administrationsagenten

Es wird dringend empfohlen, für die Ausführung des klmover-Tools und das Entfernen des Administrationsagenten den Kennwortschutz zu aktivieren. Um den Kennwortschutz zu aktivieren, wählen Sie in den Richtlinieneinstellungen des Administrationsagenten die Option **Deinstallationskennwort verwenden**.

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

Das Dienstprogramm klmover wird nur zum Verschieben von verwalteten Geräten verwendet, die von einem virtuellen Administrationsserver verwaltet werden. Bei der Installation des Administrationsagenten auf dem verwalteten Client-Gerät wird das klmover-Tool automatisch in den Installationsordner des Administrationsagenten kopiert.

Verwenden von Kaspersky Security Network

Wir empfehlen, in allen Richtlinien der verwalteten Anwendungen und in den Eigenschaften von Kaspersky Next Expert View die Verwendung von Kaspersky Security Network (KSN) zu aktivieren und die KSN-Erklärung zu akzeptieren. Wenn Sie Kaspersky Next Expert View aktualisieren, können Sie die aktualisierte KSN-Erklärung akzeptieren.

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.

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

Um rechtzeitig auf Notfälle reagieren zu können, empfehlen wir, Kaspersky Next Expert View so zu konfigurieren, dass es Benachrichtigungen über die von ihr 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.

Sicherheitsempfehlungen für Drittanbieter-Informationssysteme

Sicherheitsempfehlungen für CIS-Benchmarks

Wenn Sie Versionen von Betriebssystemen oder Virtualisierungsplattformen verwenden, die vom Administrationsagenten unterstützt werden, empfehlen wir Ihnen, sofern vorhanden, die bewährten Verfahren für Informationssicherheit des Center for Internet Security (CIS) anzuwenden, um diese Informationssysteme besser abzustimmen.

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 vom Administrationsagenten unterstützten Informationssysteme:

- 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

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.

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 eines Unternehmens gegen den 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.

Cyberbedrohungen erkennen und darauf reagieren

Um die IT-Infrastruktur eines Unternehmens wirksam vor komplexen Cyber-Bedrohungen zu schützen und die automatische Erkennung und Analyse von Sicherheitsvorfällen zu ermöglichen, empfehlen wir die Verwendung der Detection and Response-Funktionen folgender Kaspersky-Lösungen, die in die Schnittstelle der Kaspersky Next Expert View integriert werden können:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Expert

Benutzeroberfläche von Kaspersky Next Expert View

Kaspersky Next Expert View wird über eine Weboberfläche verwaltet.

Das Hauptfenster des Programms enthält die folgenden Elemente:

- Hauptmenü im linken Teil des Fensters
- Oberer Bereich im oberen Teil des Fensters
- Arbeitsbereich im rechten Fensterbereich

Hauptmenü

Das Hauptmenü enthält die folgenden Abschnitte:

- **Konsolen-Navigation**. Zeigt eine Übersicht des Hauptmenüs an. Die meisten der angezeigten Abschnitte können den Lesezeichen hinzugefügt oder als Startseite festgelegt werden. Der Abschnitt **Konsolen-Navigation** ist standardmäßig als Startseite festgelegt.
- **Administrationsserver**. Zeigt den Namen des Administrationsservers an, mit dem Sie aktuell verbunden sind. Klicken Sie auf den Namen des Administrationsservers, um die Eigenschaften des Administrationsservers zu öffnen.
- **Überwachung**. Bietet Ihnen einen Überblick über die Infrastruktur, den Schutzstatus und die Statistiken.
- **Asset-Verwaltung**. Enthält Werkzeuge für die Verwaltung von Client-Geräten, sowie von Aufgaben und Richtlinien für Kaspersky-Anwendungen.
- **Benutzer und Rollen**. Erlaubt Ihnen Benutzer und Rollen zu verwalten, Benutzerrechte durch das Zuweisen von Rollen an Benutzer zu konfigurieren und Richtlinienprofile mit Rollen zu verknüpfen.
- **Vorgänge**. Enthält eine Vielzahl von Vorgängen, wie die Lizenzierung des Programms, das Patch-Management und die Verwaltung von Drittanbieter-Anwendungen. Dies umfasst auch den Zugriff auf die Datenverwaltungen des Programms.
- **Gerätesuche und Bereitstellung**. Ermöglicht Ihnen das Durchführen von Netzwerkabfragen zum Auffinden von Client-Geräten sowie die manuelle oder automatische Verteilung dieser Geräte an Administrationsgruppen. Dies umfasst auch den Schnellstartassistenten und den Assistenten für die Bereitstellung des Schutzes.
- **Marketplace**. Enthält Informationen über den kompletten Umfang an Business-Lösungen von Kaspersky und ermöglicht es Ihnen, die erforderlichen Lösungen auszuwählen und anschließend auf der Kaspersky-Website zu erwerben.
- **Einstellungen**. Enthält Einstellungen zur Integration Kaspersky Next Expert View mit anderen Kaspersky-Anwendungen. Enthält auch Ihre persönlichen Einstellungen für das Design der Benutzeroberfläche, z. B. Sprache der Benutzeroberfläche oder das Farbschema.

Bei Bedarf können Sie das Hauptmenü durch Klicken auf das Chevron-Symbol (<<) am unteren Bildschirmrand minimieren.

Oberer Bereich

Der obere Bereich wird immer in allen Abschnitten der Konsole angezeigt und kann nicht ausgeblendet werden.

Die linke Seite des Bereichs enthält den Namen und das Logo der Anwendung. Wenn Sie auf den Namen oder das Logo der Anwendung klicken, öffnet sich die Startseite von Kaspersky Next Expert View.

In der Mitte des Bereichs befindet sich die Dropdown-Liste mit dem Namen Ihres aktuellen Arbeitsbereichs. Wenn Sie auf die Dropdown-Liste klicken und eines der Elemente auswählen, können Sie eine der folgenden Aktionen ausführen:

- Zu einem anderen Arbeitsbereich wechseln, falls verfügbar.
- Zur Liste der Arbeitsbereiche zurückkehren.

Auf der rechten Seite des Bereichs wird das Menü Ihres Benutzerkontos angezeigt. Sie können das Menü öffnen, indem Sie auf Ihren Kontonamen klicken, und anschließend einen der folgenden Schritte ausführen, indem Sie das entsprechende Element aus der Dropdown-Liste auswählen:

- Ihre Kontoeinstellungen verwalten.

  Wenn Sie den Eintrag **Benutzerkonto verwalten** auswählen, werden Sie zum Kaspersky Account Portal weitergeleitet, wo Sie Ihr Kennwort oder Ihre E-Mail-Adresse ändern sowie die Zwei-Faktor-Authentifizierung einrichten können.

- Wählen Sie die Sprache der Benutzeroberfläche von Kaspersky Next Expert View.
- Das helle Design der Benutzeroberfläche auswählen.
- Informationen zum Technischen Support von Kaspersky anzeigen.
- Zur Online-Hilfe von Kaspersky Next Expert View wechseln.
- Videos zur Konfiguration und Verwendung von Kaspersky Next Expert View und den Sicherheitsanwendungen anschauen.

  Wenn Sie im Browser Mozilla Firefox ein Video aus dem Abschnitt **Tutorials** im Pop-up-Fenster abspielen und anschließend das Video im "Bild-im-Bild"-Modus öffnen, wird das Video im "Bild-im-Bild"-Modus beim Schließen des Videos im Pop-up-Fenster ebenfalls geschlossen.

- Informationen zu rechtlichen Dokumenten für Ihre verfügbaren Kaspersky-Anwendungen anzeigen.
- Melden Sie sich von Kaspersky Next Expert View ab.

Arbeitsbereich

Im Arbeitsbereich werden die Informationen angezeigt, die Sie in den linken Abschnitten der Weboberfläche ausgewählt haben. Er enthält außerdem Steuerelemente, mit denen Sie die Darstellung der Informationen konfigurieren können.

Sprache und Farbschema der Benutzeroberfläche ändern

Sie können die Sprache und das Farbschema von Kaspersky Next Expert View auswählen.

So ändern Sie die Sprache der Benutzeroberfläche:

1. Klicken Sie im oberen Teil des Fensters auf den Namen Ihres Benutzerkontos.
   Das Menü Ihres Benutzerkontos wird angezeigt.
2. Wählen Sie in der Dropdown-Liste eine der unterstützten Sprachen aus.

Die Sprache der Benutzeroberfläche wird geändert.

So ändern Sie das Farbschema der Benutzeroberfläche:

1. Klicken Sie im oberen Teil des Fensters auf den Namen Ihres Benutzerkontos.
   Das Menü Ihres Benutzerkontos wird angezeigt. Standardmäßig ist das **Helles Design** ausgewählt.
2. Wählen Sie eines der unterstützten Farbschemas aus der Dropdown-Liste aus.

Das Farbschema der Benutzeroberfläche wurde geändert.

Startseite der Kaspersky Next Expert View anpassen

Die Startseite wird angezeigt, nachdem Sie sich an der Kaspersky Next Expert View angemeldet haben.

Standardmäßig ist die Registerkarte **Einstellungen der Startseite** des Abschnitts Konsolen-Navigation als Startseite festgelegt. Bei Bedarf können Sie die Startseite anpassen.

So passen Sie die Startseite an:

1. Bewegen Sie im Abschnitt **Konsolen-Navigation** den Mauszeiger über das Element, das Sie als Startseite festlegen möchten.

2. Wenn das Homepage-Symbol (⌂) erscheint, klicken Sie es an.

   Die Startseite ändert sich und es wird eine entsprechende Meldung auf dem Bildschirm angezeigt. Das als Startseite ausgewählte Element wird mit dem Homepage-Symbol (⌂) versehen.

Die Abschnitte **Marketplace** und **Einstellungen** können nicht als Startseite festgelegt werden.

Lesezeichen hinzufügen und entfernen

Sie können häufig aufgerufene Abschnitte von Kaspersky Next Expert View zu den Lesezeichen hinzuzufügen und diese anschließend über den Abschnitt **Lesezeichen** des Hauptmenüs schnell aufrufen.

Wenn Sie den Lesezeichen keinen Abschnitt hinzugefügt haben, wird der Abschnitt **Lesezeichen** im nicht Hauptmenü angezeigt.

Lesezeichen können für jene Abschnitte hinzugefügt werden, die Seiten enthalten und anzeigen. Wenn Sie beispielsweise den Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** aufrufen, wird die Seite mit der Gerätetabelle geöffnet. Dies bedeutet, dass Sie den Abschnitt **Assets (Geräte)** den Lesezeichen hinzufügen können. Sollte jedoch nach der Auswahl eines Abschnitts im Hauptmenü ein Fenster oder gar kein Element angezeigt werden, können Sie diesen Abschnitt nicht zu den Lesezeichen hinzufügen.

So fügen Sie einen Abschnitt zu den Lesezeichen hinzu:

1. Bewegen Sie den Mauszeiger im Hauptmenü über den Abschnitt, den Sie den Lesezeichen hinzufügen möchten.

2. Wenn ein Lesezeichen-Symbol (🔖) erscheint, klicken Sie auf das Symbol.

   Der Abschnitt wird im Bereich **Lesezeichen** angezeigt.

So entfernen Sie einen Abschnitt aus den Lesezeichen:

1. Rufen Sie im Hauptmenü den Abschnitt **Lesezeichen** auf.

2. Bewegen Sie den Mauszeiger über den Abschnitt, den Sie entfernen möchten, und klicken Sie anschließend auf das Lesezeichen-Symbol (🔖).

   Der Abschnitt wird aus den Lesezeichen entfernt.

Sie können auch im Abschnitt **Konsolen-Navigation** Elemente zu den Lesezeichen hinzufügen, bzw. aus diesen entfernen. Bewegen Sie dazu den Mauszeiger über das gewünschte Element und klicken Sie auf das Lesezeichen-Symbol (). Das ausgewählte Element wird mit dem Lesezeichen-Symbol () markiert und im Hauptmenü unter dem Abschnitt **Lesezeichen** angezeigt. Wenn Sie den Abschnitt aus den Lesezeichen entfernen möchten, klicken Sie auf das Lesezeichen-Symbol ().

Der Abschnitt **Lesezeichen** wird nur im Hauptmenü angezeigt. Er wird nie auf der Seite **Konsolen-Navigation** angezeigt.

Zur Liste mit den Arbeitsbereichen zurückkehren

Nachdem Sie Ihren Arbeitsbereich geöffnet haben, können Sie zu der Portal-Seite zurückkehren, auf der die von Ihnen angelegten Arbeitsbereiche angezeigt werden. Wenn Administratoren anderer Arbeitsbereiche Ihnen Zugriff gewährt haben, indem sie Ihrem Benutzerkonto die Rollen "Betrachter" oder "Administrator" zuweisen, werden diese Arbeitsbereiche ebenfalls auf Ihrer Portal-Seite angezeigt.

So kehren Sie zur Liste der Arbeitsbereiche zurück:

1. Klicken Sie im oberen Bereich auf die Dropdown-Liste mit dem Namen Ihres aktuellen Arbeitsbereichs.
2. Wählen Sie **Zum Portal wechseln** aus.

Die Portal-Seite zeigt die Liste der Arbeitsbereiche an.

Erstkonfiguration von Kaspersky Next Expert View

Dieser Abschnitt beschreibt das Hauptszenario für die Bereitstellung von Kaspersky Next Expert View, beginnend mit der Erstellung eines Arbeitsbereiches und endend mit der Überwachung des Netzwerkschutzstatus.

Informationen zur Bereitstellung eines lokal ausgeführten Kaspersky Security Centers finden Sie in der Kaspersky Security Center Online-Hilfe.

Wir empfehlen, dass Sie mindestens einen Werktag für die Implementierung dieses Szenarios einplanen.

Das Szenario führt Sie durch die folgenden Schritte:

- Erste Schritte für Administratoren in einem Arbeitsbereich
- Ermitteln der Geräte in Ihrem Netzwerk (Bei Bedarf weisen Sie Verteilungspunkte zu und installieren Programmpakete manuell auf den Verteilungspunkten)
- Bereitstellung verwalteter Kaspersky-Anwendungen auf den Client-Geräten und die Konfiguration der Tools, die dem Netzwerkschutz, der Überwachung und der regelmäßigen Aktualisierung der Kaspersky-Datenbanken, Software-Module und -Anwendungen dienen

Wenn Sie dieses Szenario abschließen, wird der auf Kaspersky-Anwendungen basierende Netzwerkschutz konfiguriert. Sie können weiterhin den Schutzstatus des Netzwerks überwachen.

Erforderliche Vorrausetzungen

Vor dem Start:

- Sehen Sie sich die Architektur von Kaspersky Next Expert View an, um die Interaktion zwischen den wichtigsten Programmkomponenten zu verstehen.
- Lesen Sie die Informationen zur Lizenzierung von Kaspersky Next Expert View und von verwalteten Programmen.
- Achten Sie darauf, dass Sie über einen gültigen Aktivierungscode für Kaspersky Next Expert View verfügen (wenn Sie einen kommerziellen Arbeitsbereich erstellen).

Schritte

Die Konfiguration der Kaspersky Next Expert View erfolgt schrittweise:

1. **Konfiguration der Ports**

   Vergewissern Sie sich, dass alle notwendigen Ports für die Interaktion zwischen Netzwerk und Kaspersky-Infrastruktur geöffnet sind. Wenn Sie planen, eine Hierarchie der Administrationsserver zu verwenden, stellen Sie ebenfalls sicher, dass alle notwendigen Ports für die Interaktion zwischen dem oder den sekundären Administrationsserver(n) und den Client-Geräten geöffnet sind.

2. **Einen Arbeitsbereich erstellen**

   Legen Sie ein Konto an und erstellen Sie anschließend einen Arbeitsbereich.

3. **Den Schnellstartassistenten ausführen**

   Öffnen Sie Kaspersky Next Expert View und melden Sie sich an. Wenn Sie sich zum ersten Mal anmelden, werden Sie automatisch dazu aufgefordert, den Schnellstartassistenten auszuführen. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

   Wenn der Schnellstartassistent abgeschlossen ist, stehen Ihnen Installationspakete mit Administrationsagenten und Sicherheitsanwendungen zur Verfügung. Diese Installationspakete werden für die weitere Bereitstellung von Kaspersky Next Expert View benötigt.

4. **Bereitstellung von Kaspersky-Anwendungen**

   Führen Sie das Szenario zur ersten Bereitstellung von Kaspersky-Anwendungen durch. Einer der Szenario-Schritte bezieht sich auf den Netzwerkabfragevorgang. Dieser Vorgang ist erforderlich, um Client-Geräte in Ihrem Netzwerk zu erkennen. Die Netzwerkabfrage und ihre Einstellungen sind im Szenario der Erkennung von vernetzten Geräten beschrieben.

5. **Lizenzierung von Kaspersky-Sicherheitsanwendungen**

   Wenn Kaspersky-Sicherheitsanwendungen auf den verwalteten Geräten bereitgestellt werden, muss jede Anwendung durch Verwenden eines Aktivierungscodes lizenziert werden. Stellen Sie Ihre Aktivierungscodes für die Kaspersky-Anwendungen bereit, die auf den verwalteten Geräten installiert sind. Sie haben mehrere Möglichkeiten, Kaspersky Sicherheitsanwendungen zu lizenzieren.

6. **Netzwerkschutz konfigurieren**

   Führen Sie die Konfiguration des Netzwerkschutzes durch, um die mit dem Schnellstartassistenten erstellten Richtlinien und Aufgaben zu optimieren. Achten Sie darauf, die Auslastung der Anwendungen zum Endpunktschutz zu optimieren.

7. **Regelmäßiges Aktualisieren der Datenbanken, Softwaremodule und Programme von Kaspersky**

   Um Ihr Netzwerk vor Viren und anderen Bedrohungen zu schützen, müssen Sie regelmäßige Updates für die Datenbanken, Softwaremodule und Programmen von Kaspersky konfigurieren.

8. **Aktualisieren von Drittanbieter-Programmen und Schließen von Schwachstellen in Drittanbieter-Programmen (optional)**

   Kaspersky Next Expert View ermöglicht die Verwaltung von Updates für Microsoft-Programme, die auf Client-Geräten installiert sind. Sie können auch Schwachstellen in Microsoft-Programmen schließen, indem Sie die erforderlichen Updates installieren.

9. **Konfigurieren von Tools zur Überwachung des Netzwerkschutzstatus**

   Wählen und konfigurieren Sie Widgets, Berichte und andere Tools, mit denen Sie den Status des Netzwerkschutzes überwachen können.

Wenn die Kaspersky Next Expert View bereitgestellt und konfiguriert ist, können Sie mit der Überwachung des Netzwerkschutzstatus fortfahren.

Szenario: Erstellen einer Hierarchie von Administrationsservern, die durch Kaspersky Next Expert View verwaltet wird

In diesem Szenario werden die Abläufe beschrieben, die Sie ausführen müssen, um eine Hierarchie von Administrationsservern zu erstellen, die durch Kaspersky Next Expert View verwaltet wird. Kaspersky Next Expert View übernimmt somit die Rolle des primären Administrationsservers. Diese Hierarchie kann anschließend für die Migration verwalteter Geräte und Objekte von Kaspersky Security Center auf Kaspersky Next Expert View, sowie für die Verwaltung von sekundären Administrationsservern und Geräten durch Kaspersky Next Expert View verwendet werden.

Kaspersky Next Expert View kann nur als primärer Administrationsserver fungieren, während lokal ausgeführte Administrationsserver nur als sekundäre Administrationsserver fungieren können. Andere hierarchische Strukturen sind nicht verfügbar.

Erforderliche Vorrausetzungen

Stellen Sie vor dem Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der lokal ausgeführte Administrationsserver wurde auf Version 12 oder höher aktualisiert.
- Die Kaspersky Security Center Web Console wurde auf dem lokalen Administrationsserver installiert.
- Die Web-Plug-ins, für die Programme, die Sie durch Kaspersky Next Expert View verwalten möchten, wurden installiert.
- Die verwalteten Anwendungen wurden auf Versionen aktualisiert, die von Kaspersky Next Expert View unterstützt werden.
- Stellen Sie sicher, dass in der Aufgabe zum "Download von Updates in die Datenverwaltung des Administrationsservers" auf dem lokal ausgeführten Administrationsserver nicht der primäre Administrationsserver als Update-Quelle zugewiesen ist. Ändern Sie gegebenenfalls die Aufgabeneinstellungen entsprechend.

Nach dem Erstellen der Hierarchie werden die in Kaspersky Next Expert View wirksamen Richtlinien und Aufgaben auf den sekundären Administrationsserver angewendet, wodurch dessen vorhandenen Richtlinien und Aufgaben ersetzt werden. Wenn Sie dieses Verhalten vermeiden möchten, löschen Sie in Kaspersky Next Expert View alle Richtlinien und Aufgaben, bevor Sie die Hierarchie erstellen. Alternativ können Sie den Status jeder Richtlinie in Kaspersky Next Expert View in ihren Einstellungen auf **Inaktiv** ändern, und in den Einstellungen für jede Aufgabe in Kaspersky Next Expert View die Option **An sekundäre und virtuelle Administrationsserver verteilen** deaktivieren.

Falls notwendig, ist das Löschen Ihrer Hierarchie von Administrationsservern jederzeit möglich.

Schritte der Hierarchieerstellung

Das Basisszenario sieht einen sekundären Administrationsserver vor, auf den nicht über das Internet zugegriffen werden kann. Die Vorgänge in einigen der unten beschriebenen Schritte können jedoch davon abweichen, wenn auf den sekundären Administrationsserver über das Internet zugegriffen werden kann. Außerdem müssen in diesem Fall einige Schritte übersprungen werden.

Die Erstellung einer Hierarchie von Administrationsservern umfasst die folgenden Schritte:

1. **Abrufen des Zertifikats des sekundären Administrationsservers**

   Wenn der sekundäre Administrationsserver über das Internet erreichbar ist, überspringen Sie diesen Schritt.

   Öffnen Sie in der lokal ausgeführten Kaspersky Security Center Web Console die Eigenschaften des Administrationsservers und öffnen Sie auf der Registerkarte **Allgemein** den Abschnitt **Allgemein**. Klicken Sie auf den Link **Zertifikat des Administrationsservers anzeigen**. Die Zertifikatsdatei wird im cer-Format automatisch in dem Ordner gespeichert, der in den Einstellungen Ihres Browsers angegeben ist.

2. **Abrufen der Verbindungseinstellungen und Zertifikate von der Kaspersky Next Expert View**

   Wenn der sekundäre Administrationsserver über das Internet erreichbar ist, überspringen Sie diesen Schritt.

   Öffnen Sie in Kaspersky Next Expert View die Eigenschaften des Administrationsservers und öffnen Sie auf der Registerkarte **Allgemein** den Abschnitt **Hierarchie der Administrationsserver**. Die folgenden Verbindungseinstellungen werden angezeigt:

   - **HDS-Adresse**

     Zeigt die Webadresse an, die für die Verbindung mit dem Hosted Discovery Service (HDS) verwendet wird.

   - **HDS-Port**

     Zeigt die Nummer des Ports an, der für die Verbindung mit HDS verwendet wird.

   Zusätzlich sind in dem Abschnitt zwei Links enthalten:

   - **Zertifikat des Administrationsservers anzeigen**

     Durch Klicken auf diesen Link wird der öffentliche Schlüssel des Instanz-Zertifikats von Kaspersky Next Expert View heruntergeladen.

   - **HDS Root CA-Zertifikat**

     Durch Klicken auf diesen Link wird die Datei im pem-Format heruntergeladen, die eine Liste von durch Zertifizierungsstellen (Root Certificate Authorities - CA) ausgestellten vertrauenswürdigen Stamm-Zertifikaten enthält. Diese Datei ist für die Verwendung durch den sekundären Administrationsserver vorgesehen: Dieser muss das HDS-Zertifikat überprüfen.

Kopieren Sie die Verbindungseinstellungen manuell – mithilfe der Zwischenablage oder auf eine beliebige andere Weise – und speichern Sie diese in einer Datei in einem beliebigen Format. Klicken Sie auf den Link **Zertifikat des Administrationsservers anzeigen** und warten Sie, bis die Zertifikatdatei heruntergeladen wurde. Klicken Sie auf den Link **HDS Root CA-Zertifikat** und warten Sie, bis die Datei mit den durch Zertifizierungsstellen ausgestellten vertrauenswürdigen Stamm-Zertifikaten heruntergeladen wurde. Beide Dateien werden in dem Ordner gespeichert, der in Ihren Browsereinstellungen angegeben ist.

3. **Auswählen des sekundären Administrationsservers für die Verbindung**

   Wechseln Sie in den Eigenschaften des Administrationsservers auf die Registerkarte **Administrationsserver**. Aktivieren Sie in der Hierarchie der Administrationsgruppen das Kontrollkästchen neben der Administrationsgruppe, die den sekundären Administrationsserver mit all seinen verwalteten Geräten enthalten soll. Klicken Sie auf die Schaltfläche **Sekundären Administrationsserver verbinden**.

   Geben Sie auf der sich öffnenden Seite im Feld **Anzeigename des sekundären Administrationsservers** den Namen an, unter dem der sekundäre Administrationsserver in der Hierarchie angezeigt werden soll. Dies dient nur der Zugänglichkeit und daher kann der Name bei Bedarf vom tatsächlichen Namen des sekundären Administrationsservers abweichen. Klicken Sie auf die Schaltfläche **Weiter**.

   > Wenn der sekundäre Administrationsserver über das Internet erreichbar ist, müssen Sie die Adresse des sekundären Administrationsservers zusätzlich im Feld **Adresse des sekundären Administrationsservers (optional)** angeben.

   Klicken Sie auf der nächsten Seite auf die Schaltfläche **Durchsuchen** und geben Sie die pem-Datei an, die Sie vom sekundären Administrationsserver heruntergeladen haben. Klicken Sie auf die Schaltfläche **Weiter**.

4. **Proxyserver aktivieren und konfigurieren**

   > Die in diesem Schritt beschriebenen Aktionen sind optional. Führen Sie diese nur aus, wenn für Ihre Verbindung ein Proxyserver erforderlich ist.

   Klicken Sie auf die Schaltfläche **Weiter**. Auf der Seite **Verbindungs- und Authentifizierungseinstellungen** können Sie die Verwendung von Proxy-Servern konfigurieren, falls notwendig. Aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie die folgenden Einstellungen an:

   - **Proxyserver-Adresse**

     Die Adresse des Proxyservers.

   - **Benutzername**

     Der Benutzername für die Anmeldung am Proxyserver.

   - **Kennwort**

     Das Kennwort für die Anmeldung am Proxyserver.

5. **Festlegen der Authentifizierungseinstellungen und hinzufügen des sekundären Administrationsservers zur Hierarchie**

   Klicken Sie auf die Schaltfläche **Weiter**. Geben Sie auf der Seite **Anmeldedaten des sekundären Administrationsservers** die folgenden Einstellungen an:

   - **Benutzername**

     Der Benutzername für die Anmeldung am sekundären Administrationsserver.

- **Kennwort**

  Das Kennwort für die Anmeldung am sekundären Administrationsserver.

Klicken Sie auf **Weiter** und warten Sie, bis der sekundäre Administrationsserver in der Hierarchie angezeigt wird.

Wenn der sekundäre Administrationsserver über das Internet erreichbar ist, verbindet er sich mit dem primären Administrationsserver.

> Wenn der sekundäre Administrationsserver über das Internet erreichbar ist und die Verbindung zwischen den beiden Administrationsservern erfolgreich hergestellt werden konnte, ignorieren Sie alle weiteren Schritte.

Wenn der sekundäre Administrationsserver nicht über das Internet erreichbar ist, wird dieser zwar sichtbar, aber Sie müssen zusätzliche Maßnahmen ergreifen, um Kontrolle über den sekundären Administrationsserver zu erlangen.

6. **Konfigurieren der Verbindung in der lokal ausgeführten Kaspersky Security Center Web Console**

   Öffnen Sie in der lokal ausgeführten Kaspersky Security Center Web Console die Eigenschaften des Administrationsservers und öffnen Sie auf der Registerkarte **Allgemein** den Abschnitt **Hierarchie der Administrationsserver**. Aktivieren Sie das Kontrollkästchen **Dieser Administrationsserver ist in der Server-Hierarchie sekundär**. Wählen Sie in der Liste **Typ des primären Administrationsservers** die Option **Kaspersky Security Center Cloud Console**.

   > Kaspersky Security Center Web Console prüft, ob der primäre Administrationsserver als Update-Quelle in der *Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers* angegeben wurde. Wurde der primäre Administrationsserver als Update-Quelle angegeben, erhalten Sie eine entsprechende Meldung mit einer Warnung und einen Link zu den Aufgabeneinstellungen. Sie können die Einstellungen anpassen und danach zur Erstellung der Hierarchie zurückkehren, oder Sie überspringen den Schritt und fahren mit der Erstellung der Hierarchie fort.

   Geben Sie in der Gruppe **Einstellungen für den Verbindungsaufbau zwischen dem sekundären und dem primären Administrationsserver** die folgenden Einstellungen an:

   - **Adresse des HDS-Servers (des primären Administrationsservers in Cloud Console)**

     Geben Sie die Adresse des HDS im Format des vollqualifizierten Domänennamens (FQDN) ein, den Sie aus den Einstellungen des Administrationsservers in Kaspersky Next Expert View kopiert und gespeichert haben.

   - **Ports des HDS-Servers**

     Geben Sie Nummer(n) des/der HDS-Serverports an, den/die Sie aus den Einstellungen des Administrationsservers in Kaspersky Next Expert View kopiert und gespeichert haben.

7. **Hinzufügen der Zertifikate zum sekundären Administrationsserver**

   Klicken Sie auf **Zertifikat des primären Administrationsservers angeben** und geben Sie die Zertifikats-Datei an, die Sie aus den Einstellungen des Administrationsservers in Kaspersky Next Expert View gespeichert haben.

   Klicken Sie auf **Zertifikate des Hosted Discovery Service angeben** und geben Sie die pem-Datei an, die Sie aus den Einstellungen des Administrationsservers in Kaspersky Next Expert View gespeichert haben.

   > Wenn Sie bei der Verbindung des sekundären Administrationsservers in Kaspersky Next Expert View die Verwendung eines Proxyservers aktiviert haben, wählen Sie das Kontrollkästchen **Proxyserver verwenden** aus und geben Sie die gleichen Proxyeinstellungen wie in Kaspersky Next Expert View an.

Sie können ebenfalls das Kontrollkästchen **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden** aktivieren, wenn sich der sekundäre Administrationsserver in einer demilitarisierten Zone (DMZ) befindet.

Der sekundäre Administrationsserver verbindet sich mit dem primären Administrationsserver.

Ergebnisse

Nach dem Ausführen der obigen Schritte, können Sie folgendermaßen überprüfen, ob die Hierarchie erfolgreich erstellt wurde:

- Die aktiven Richtlinien des primären Administrationsservers sind auch auf dem sekundären Administrationsserver aktiv. Die Aufgaben des primären Administrationsservers wurden auf den sekundären Administrationsserver verteilt. Wenn die Option **An sekundäre und virtuelle Administrationsserver verteilen** in den Einstellungen einer Gruppenaufgabe aktiviert wurde, wird jede dieser Aufgaben ebenso auf den sekundären Administrationsserver verteilt.

- Richtlinieneinstellungen, die auf dem primären Administrationsserver vor Anpassungen gesperrt wurden, werden in allen Richtlinien auf dem sekundären Administrationsserver als gesperrt angezeigt.

- Die vom primären Administrationsserver angewandten Richtlinien werden in dem sekundären Administrationsserver in der Liste der Richtlinien angezeigt (**Asset-Verwaltung→ Richtlinien**).

- Die vom primären Administrationsserver verteilten Gruppenaufgaben werden in dem sekundären Administrationsserver in der Liste der Aufgaben angezeigt (**Asset-Verwaltung → Aufgaben**).

- Richtlinien und Aufgaben, die auf dem primären Administrationsserver erstellt wurden, können in dem sekundären Administrationsserver nicht angepasst werden.

- In Kaspersky Next Expert View wird der sekundäre Administrationsserver innerhalb der Struktur der Administrationsgruppen in der Gruppe angezeigt, die Sie beim Hinzufügen dieses Administrationsservers festgelegt haben.

Migration nach Kaspersky Next Expert View

Dieser Abschnitt beschreibt den Vorgang für die Migration von verwalteten Geräten und zugehörigen Objekten von einer lokal ausgeführten Kaspersky Security Center Web Console der Version 12 (oder höher) auf Kaspersky Next Expert View.

Methoden der Migration auf Kaspersky Next Expert View

Mit der Migrationsfunktion können Sie vernetzte Geräte aus Kaspersky Security Center unter die Verwaltung von Kaspersky Next Expert View stellen. Ihre verwalteten Geräte werden umgeschaltet, ohne dabei prinzipielle Einstellungen wie die Administrationsgruppenzugehörigkeit, oder grundlegende Objekte wie die Richtlinien und Aufgaben mit Bezug auf die verwalteten Programme, zu verlieren.

Sie können aus zwei zur Verfügung stehenden Methoden für die Migration Ihres Administrationsservers in Kaspersky Next Expert View auswählen:

- Migration ohne Hierarchie von Administrationsservern:
  - Macht den Wechsel der verwalteten Geräte und zugehörigen Objekten zu Kaspersky Next Expert View selbst dann möglich, wenn der lokal ausgeführte Administrationsserver kein sekundärer Server in Bezug auf Kaspersky Next Expert View ist.
  - Es kann das Übertragen von Daten notwendig sein (via Wechseldatenträger, E-Mails, eines gemeinsamen Ordners oder auf eine andere beliebige Weise), wenn Kaspersky Security Center Web Console und Kaspersky Next Expert View auf unterschiedlichen physischen Geräten geöffnet sind.

  Sie können außerdem eine Migration mit virtuellen Administrationsservern durchführen, wenn diese in Ihrem Netzwerk vorhanden sind.

- Migration unter Verwendung einer Hierarchie von Administrationsservern:
  - Macht den Wechsel der verwalteten Geräte und zugehörigen Objekte zu Kaspersky Next Expert View durch ausschließliche Verwendung der Benutzeroberfläche von Kaspersky Next Expert View möglich. Es wird daher kein physisches Übertragen von Daten benötigt.
  - Dies setzt voraus, dass der lokal ausgeführte Administrationsserver als sekundärer Server von Kaspersky Next Expert View fungiert. Sie können eine derartige Hierarchie vor dem Beginn der Migration erzeugen.

Für die vollständige Festplattenverschlüsselung wird von Kaspersky Next Expert View nur BitLocker unterstützt.

Szenario: Migration ohne Administrationsserver-Hierarchie

Dieser Abschnitt beschreibt die Migration von verwalteten Geräten und zugehörigen Objekten (wie Richtlinien, Aufgaben und Berichte) von einem lokal ausgeführten Kaspersky Security Center Web Console auf Kaspersky Next Expert View. Sie können eine einzelne Administrationsgruppe in den Migrationsbereich aufnehmen, um dieselbe Administrationsgruppe in Kaspersky Next Expert View wiederherzustellen.

Diese Gruppe muss die verwalteten Geräte eines einzelnen Betriebssystems enthalten. Wenn Ihr Netzwerk über Geräte mit unterschiedlichen Betriebssystemen oder Linux-Distributionen verfügt, ordnen Sie diese Geräte verschiedenen Administrationsgruppen zu und migrieren Sie anschließend jede Gruppe separat.

Nach Abschluss der Migration sind alle Administrationsagenten innerhalb des Migrationsbereichs aktualisiert und werden über Kaspersky Next Expert View verwaltet.

> Die Schritte in diesem Abschnitt erklären die Durchführung des Migrationsprozesses, wenn keine Hierarchie von Administrationsservern besteht. Dies bedeutet, dass noch keine Verbindung zwischen Kaspersky Next Expert View und der lokal ausgeführten Kaspersky Security Center Web Console bestanden hat.

Erforderliche Vorrausetzungen

Erfüllen Sie zunächst die folgenden Voraussetzungen:

- Der lokal ausgeführte Administrationsserver wurde auf Version 14.2 oder höher aktualisiert.
- Installation von Kaspersky Security Center Web Console in Version 12.1 oder höher.
- Aktualisieren Sie die Administrationsagenten auf den verwalteten Geräten auf die Version 12 oder höher.
- Verwenden Sie auf Windows-Geräten den Administrationsagenten ohne Kennwort für die Deinstallation.

  Wenn das Kennwort bereits festgelegt wurde, führen Sie in der Kaspersky Security Center Web Console einen der folgenden Schritte aus:

  - Deaktivieren Sie die Option **Deinstallationskennwort verwenden** in den Richtlinieneinstellungen des Administrationsagenten.
  - Führen Sie unter Verwendung der Aufgabe *Remote-Deinstallation einer Anwendung* eine Remote-Deinstallation des Administrationsagenten durch. Wählen Sie im Feld **Zu deinstallierende Anwendung** der Aufgabe das Programm **Kaspersky Security Center Administrationsagent** aus. Vergessen Sie nicht, das Kennwort für die Deinstallation einzugeben.
- Aktualisieren Sie die verwalteten Programme auf Versionen, die von Kaspersky Next Expert View unterstützt werden.
- Stellen Sie sicher, dass Sie über Richtlinien für die neuesten Versionen des verwalteten Programms verfügen. Wenn Sie veraltete Richtlinien verwenden, erstellen Sie neue Richtlinien für die Versionen der Anwendung, die von Kaspersky Next Expert View unterstützt werden.

- Um aktuelle Richtlinien zu verwenden, aktualisieren Sie die Web-Plug-ins, für die Programme, die Sie durch Kaspersky Next Expert View verwalten möchten.
- Deinstallieren Kaspersky-Anwendungen von verwalteten Geräten, wenn diese Anwendungen nicht durch Kaspersky Next Expert View unterstützt werden.
- Entschlüsseln aller Daten (auf Festplatten- oder Dateiebene), die durch Kaspersky Endpoint Security für Windows auf verwalteten Windows-Geräten verschlüsselten wurden. Deaktivieren Sie anschließend auf den verwalteten Geräten die Verschlüsselungsfunktion entweder lokal oder über eine Anwendungsrichtlinie. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

  Befinden sich auf dem verwalteten Windows-Gerät immer noch Dateien oder Ordner, die von Kaspersky Endpoint Security für Windows verschlüsselt wurden, wird das Upgrade des Administrationsagenten während des Migrationsprozesses abgebrochen. Sie werden durch eine Meldung dazu aufgefordert, alle Daten auf dem Gerät zu entschlüsseln und die Verschlüsselungsfunktion zu deaktivieren.

Kaspersky Next Expert View unterstützt maximal 25.000 verwaltete Geräte pro Administrationsserver.

Schritte der Migration

Die Migration auf Kaspersky Next Expert View umfasst die folgenden Schritte:

1. **Planen des Migrationsumfangs und Überprüfen der Voraussetzungen**

   Schätzen Sie den Umfang des Migrationsprozesses, d.h. die zu exportierende Administrationsgruppe, ein und bewerten Sie die Anzahl der darin verwalteten Geräte. Stellen Sie außerdem sicher, dass alle als Migrationsvoraussetzungen aufgeführten Aktivitäten erfolgreich abgeschlossen wurden.

2. **Exportieren verwalteter Geräte, Objekte und Einstellungen aus Kaspersky Security Center Web Console**

   Verwenden Sie den Migrationsassistenten der lokal ausgeführten Kaspersky Security Center Web Console, um Ihre verwalteten Geräte zusammen mit ihren Objekten zu exportieren.

   Die Größe der Exportdatei beträgt maximal 4 GB.

3. **Importieren der Exportdatei in Kaspersky Next Expert View**

   Übertragen Sie die Informationen über Ihre verwalteten Geräte und Objekte an Kaspersky Next Expert View. Verwenden Sie zu diesem Zweck den Migrationsassistenten der Kaspersky Next Expert View, um die Exportdatei zu importieren und ein autonomes Installationspaket für den Administrationsagenten zu erstellen.

4. **Neuinstallation des Administrationsagenten auf verwalteten Geräten**

   Kehren Sie zum Migrationsassistenten der lokal ausgeführten Kaspersky Security Center Web Console zurück, um eine Aufgabe zur Remote-Installation zu erstellen. Sie können diese Aufgabe (sofort oder später) verwenden, um den Administrationsagenten auf Ihren verwalteten Geräten erneut zu installieren und den Migrationsprozess abzuschließen.

Ergebnisse

Nach dem Abschluss der Migration kann durch folgende Punkte sichergestellt werden, dass diese erfolgreich verlaufen ist:

- Der Administrationsagent wurde auf allen verwalteten Geräten neu installiert.
- Alle Geräte werden durch Kaspersky Next Expert View verwaltet.
- Alle Objekteinstellungen, die vor der Migration wirksam waren, sind erhalten geblieben.

Migrationsassistent

Dieser Abschnitt enthält Informationen zu den Migrationsassistenten in Kaspersky Next Expert View und Kaspersky Security Center Web Console in der Version 12 oder höher.

Schritt 1. Exportieren verwalteter Geräte, Objekte und Einstellungen aus Kaspersky Security Center Web Console

Die Migration verwalteter Geräte von Kaspersky Security Center Web Console nach Kaspersky Next Expert View erfordert das Erstellen einer Exportdatei, die Informationen über die Hierarchie der Administrationsgruppe in Ihrem aktuellen lokal ausgeführten Administrationsserver enthält. Die Exportdatei muss ebenfalls Informationen über Objekte und deren Einstellungen enthalten. Die Exportdatei wird für den anschließenden Import in die Kaspersky Next Expert View verwendet.

Die Größe der Exportdatei beträgt maximal 4 GB.

Um Objekte und deren Einstellungen aus der Kaspersky Security Center Web Console zu exportieren:

1. Wechseln Sie im Hauptmenü von Kaspersky Security Center Web Console zu **Vorgänge** → **Migration**.
2. Klicken Sie auf der Begrüßungsseite des Migrationsassistenten auf **Weiter**. Die Seite **Verwaltete Geräte für den Export** wird geöffnet und zeigt die gesamte Hierarchie der Administrationsgruppen des entsprechenden Administrationsservers an.
3. Klicken Sie auf der Seite **Verwaltete Geräte für den Export** auf den das Chevron-Symbol (>) neben dem Gruppennamen **Verwaltete Geräte**, um die Hierarchie der Verwaltungsgruppen zu erweitern. Wählen Sie die Administrationsgruppe aus, die Sie exportieren möchten.

   Nach dem die Migration eines lokal ausgeführten Kaspersky Security Center zu Kaspersky Next Expert View für zwei Administrationsgruppen durchgeführt wurde, werden die Aufgaben zur Remote-Installation für diese Gruppen mit dem gleichen Namen angezeigt.

4. Wählen Sie die verwalteten Programme aus, deren Richtlinien und Aufgaben zusammen mit Gruppenobjekten an Kaspersky Next Expert View übertragen werden müssen. Um die verwalteten Programme auszuwählen, deren Objekte exportiert werden sollen, aktivieren Sie die Kontrollkästchen neben ihren Namen in der Liste.

   Der Kaspersky Security Center Administrationsserver wird zwar in der Liste aufgeführt, allerdings erfolgt bei entsprechend aktiviertem Kontrollkästchen kein Export von dessen Richtlinien.

   Um sicherzugehen, dass Ihre verwalteten Programme von Kaspersky Next Expert View unterstützt werden, klicken Sie auf den entsprechenden Link. Dieser öffnet in der Online-Hilfe einen Abschnitt mit einer Liste verwalteter Programme, die von Kaspersky Next Expert View unterstützt werden.

   > Wenn Sie Anwendungen auswählen, die von der Kaspersky Next Expert View nicht unterstützt werden, so werden die Richtlinien und Aufgaben dieser Anwendungen trotzdem exportiert und anschließend importiert. Diese können jedoch aufgrund fehlender dezidierter Plug-ins nicht in Kaspersky Next Expert View verwaltet werden.

5. Zeigen Sie die Liste der standardmäßig exportierten Gruppenobjekte an und geben Sie gegebenenfalls weitere Nicht-Gruppenobjekte an, die zusammen mit der ausgewählten Administrationsgruppe exportiert werden sollen. Konfigurieren Sie den Exportbereich, indem Sie verschiedene Objekte ein- oder ausschließen, z. B. globale Aufgaben, benutzerdefinierte Geräteauswahlen, Berichte, benutzerdefinierte Rollen, interne Benutzer und Sicherheitsgruppen sowie benutzerdefinierte Programmkategorien. Diese Seite enthält die folgenden Abschnitte:

   - **Globale Aufgaben**

     Die Liste mit den globalen Aufgaben der verwalteten Anwendungen sowie der globalen Aufgaben des Administrationsagenten.

     > Wenn eine von Ihnen ausgewählte globale Aufgabe für eine bestimmte Objektauswahl gilt, wird diese Auswahl ebenfalls exportiert.

     > Die globalen Aufgaben des Administrationsservers werden zwar in der Liste aufgeführt, allerdings können sie nicht exportiert werden. Wenn Sie diese Aufgaben auswählen, ändert sich der Exportbereich nicht. Es werden außerdem keine Aufgaben zur Remote-Installation in den Exportbereich aufgenommen, da deren zugehörigen Installationspakete nicht exportiert werden können.

   - **Geräteauswahlen**

     Die Liste mit benutzerdefinierten Geräteauswahlen.

   - **Berichte**

     Die bearbeitbare Liste mit zu exportierenden Instanzen der Berichte.

     > Wenn ein von Ihnen ausgewählter Bericht für eine bestimmte Objektauswahl gilt, wird diese Auswahl ebenfalls exportiert.

     > Da Kaspersky Next Expert View die gleichen Berichtsvorlagen wie Kaspersky Security Center Web Console enthält, können Sie nur die Berichte für den Export auswählen, die Sie manuell erstellt oder konfiguriert haben.

- **Gruppenobjekte**

  Die Liste der standardmäßig exportierten Gruppenobjekte. Die folgenden Objekte, die sich auf die ausgewählte Administrationsgruppe beziehen, werden standardmäßig vollständig exportiert:

  - Struktur der Administrationsgruppen, d. h. alle untergeordneten Gruppen der ausgewählten Administrationsgruppe.
  - Geräte, die in den zu exportierenden Administrationsgruppen enthalten sind.
  - Tags, die den zu exportierenden Geräten zugewiesen wurden.

    Wenn ein Tag in Kaspersky Security Center Web Console erstellt, aber keinem Gerät zugewiesen wurde, wird es nicht exportiert. Die Regeln für die automatische Tag-Zuweisung werden ebenfalls nicht exportiert.

  - Gruppenrichtlinien der ausgewählten verwalteten Anwendungen.

    Richtlinien des Administrationsservers und des Administrationsagenten werden nicht exportiert.

  - Gruppenaufgaben der ausgewählten verwalteten Anwendungen und des Administrationsagenten.

    Aufgaben des Administrationsservers werden nicht exportiert.

  Sie können das Exportieren bestimmter Arten von Nicht-Gruppenobjekten auch verhindern:

  - Um den Export benutzerdefinierter Rollen (d.h. nur diejenigen, die vom Benutzer erstellt wurden) abzubrechen, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Rollen vom Export ausschließen**.
  - Um den Export interner Benutzer und Sicherheitsgruppen abzubrechen, aktivieren Sie das Kontrollkästchen **Interne Benutzer und Sicherheitsgruppen vom Export ausschließen**.
  - Um den Export benutzerdefinierter Programmkategorien mit manuell hinzugefügtem Inhalt abzubrechen, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Programmkategorien vom Export ausschließen**.

Wenn Sie Geräte mit verschiedenen Betriebssystemen in die Kaspersky Next Expert View übertragen, müssen Objekte, die keiner Gruppe entsprechen, nur einmal migriert werden.

Der Migrationsassistent überprüft die Gesamtzahl der verwalteten Geräte, die in der ausgewählten Administrationsgruppe enthalten sind. Wenn diese Zahl 10.000 übersteigt, wird eine Fehlermeldung angezeigt. Die Schaltfläche **Weiter** bleibt solange inaktiv (ausgegraut), bis sich die Anzahl der verwalteten Geräte in der ausgewählten Administrationsgruppe innerhalb der Beschränkung befindet.

6. Nachdem Sie den Migrationsbereich definiert haben, klicken Sie auf **Weiter**, um den Exportvorgang zu starten. Die Seite **Exportdatei wird erstellt** wird geöffnet, auf der Sie den Exportfortschritt aller Objekttypen anzeigen können, die Sie in den Migrationsbereich aufgenommen haben. Warten Sie, bis alle Aktualisierungssymbole (🔄) neben den Elementen in der Objektliste durch grüne Häkchen (✓) ersetzt wurden. Der Exportprozess wird abgeschlossen und die Exportdatei wird automatisch in den standardmäßigen Download-Speicherort heruntergeladen, der in Ihren Browser-Einstellungen festgelegt ist. Der Name der Exportdatei wird im unteren Teil des Browserfensters angezeigt.

7. Wenn die Seite **Der Export wurde erfolgreich abgeschlossen** angezeigt wird, fahren Sie mit dem nächsten Schritt fort, der in Kaspersky Next Expert View ausgeführt wird.

Wenn Sie Kaspersky Security Center Web Console und Kaspersky Next Expert View auf verschiedenen Geräten verwenden, müssen Sie die Exportdatei auf einen Wechseldatenträger kopieren oder andere Möglichkeiten zum Übertragen der Datei auswählen.

Schritt 2. Importieren der Exportdatei in Kaspersky Next Expert View

Um aus Kaspersky Security Center Web Console exportierte Informationen zu verwalteten Geräten und Objekten mitsamt deren Einstellungen zu übertragen, müssen Sie diese in die Kaspersky Next Expert View importieren, die in Ihrem Arbeitsbereich bereitgestellt wurde. Auf diese Weise können Sie ein autonomes Installationspaket erstellen und es für die Neuinstallation des Administrationsagenten auf Ihren verwalteten Geräten verwenden.

Stellen Sie vor dem Start des Migrationsassistenten in Kaspersky Next Expert View sicher, dass dessen eingestellte Lokalisierungssprache der Sprache von Kaspersky Security Center Web Console während des Exports entspricht. Ändern Sie gegebenenfalls die Sprache.

Wenn Sie in Ihrem Arbeitsbereich von Kaspersky Next Expert View den Schnellstartassistenten bereits zuvor abgeschlossen haben, enthält die Gruppe **Verwaltete Geräte** mit Standardeinstellungen erstelle Richtlinien und Aufgaben. Löschen Sie diese Richtlinien und Aufgaben, bevor Sie die aus Kaspersky Security Center Web Console exportierten Richtlinien und Aufgaben importieren.

Um die Exportdatei in Kaspersky Next Expert View zu importieren:

1. Wechseln Sie im Hauptmenü der Kaspersky Next Expert View zu **Vorgänge** → **Migration**.

2. Klicken Sie auf der Begrüßungsseite des Migrationsassistenten auf **Importieren**. Wählen Sie im sich öffnenden Dateiexplorer die Exportdatei aus, indem Sie zu dem Ordner navigieren, in dem sie gespeichert wurde, und auf **Öffnen** klicken. Warten Sie bis das Aktualisierungssymbol (🔄) neben dem Upload-Status der Datei durch das grüne Häkchen (✓) ersetzt wurde.

3. Klicken Sie auf die Schaltfläche **Weiter**. Die nächste Seite öffnet sich und zeigt die gesamte Hierarchie der Administrationsgruppen des Administrationsservers in Kaspersky Next Expert View an.

4. Aktivieren Sie das Kontrollkästchen neben der Ziel-Administrationsgruppe, für welche die Gruppenobjekte wiederhergestellt werden sollen und klicken Sie auf **Weiter**. Der Migrationsassistent zeigt eine Liste der in Kaspersky Next Expert View verfügbaren Installationspakete des Administrationsagenten an.

5. Wählen Sie das Installationspaket mit der entsprechenden Version und Lokalisierung des Administrationsagenten aus und klicken Sie auf **Weiter**.

Wählen Sie das Installationspaket des Administrationsagenten für Windows nur aus, wenn Sie zuvor in Ihrem Arbeitsbereich von Kaspersky Next Expert View den Schnellstartassistenten abgeschlossen und die Migration der Windows-Geräte durchgeführt haben.

Warten Sie, bis der Migrationsassistent ein autonomes Installationspaket erstellt. Die maximale Dateigröße des autonomen Installationspakets für den Administrationsagenten beträgt 200 MB.

Die Datei wird entpackt und automatisch in den standardmäßigen Download-Speicherort heruntergeladen, der in Ihren Browser-Einstellungen festgelegt ist. Die Nicht-Gruppenobjekte und Gruppenobjekte werden in der Ziel-Administrationsgruppe wiederhergestellt.

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 Sie die gesamte Gruppe **Verwaltete Geräte** importiert haben, ist es empfehlenswert, dass Sie die neu importierte Untergruppe umbenennen, um Verwirrung zu vermeiden:

a. Wechseln Sie zum Abschnitt **Gruppenhierarchie**.

b. Klicken Sie in der Gruppenstruktur auf den Namen der Untergruppe.

c. Geben Sie in dem Feld **Name** des sich öffnenden Eigenschaftenfensters einen anderen Namen ein (z. B. "Migrierte Geräte").

Es wird empfohlen, zu überprüfen, ob die im Exportbereich enthaltenen Objekte (Richtlinien, Aufgaben und verwaltete Geräte) erfolgreich in die Kaspersky Next Expert View importiert wurden. Wechseln Sie dafür in den Abschnitt **Asset-Verwaltung** und prüfen Sie, ob in den Listen der Unterabschnitte **Richtlinien**, **Aufgaben**, und **Assets (Geräte)** die importierten Objekte enthalten sind.

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. Anschließend beginnen die Geräte mit dem Wechsel zu Kaspersky Next Expert View.

6. Klicken Sie auf **Fertigstellen**, um das Fenster des Migrationsassistenten zu schließen.

7. Wenn Sie das autonome Installationspaket erneut suchen und herunterladen möchten, wechseln Sie zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete** und klicken Sie auf die Schaltfläche **Liste der autonomen Pakete anzeigen**. Wählen Sie in der sich öffnenden Liste das von Ihnen erstellte autonome Installationspaket aus und klicken Sie auf die Schaltfläche **Herunterladen**.

Wenn Sie Kaspersky Security Center Web Console und Kaspersky Next Expert View auf verschiedenen Geräten verwenden, müssen Sie das autonome Installationspaket auf einen Wechseldatenträger kopieren oder andere Möglichkeiten zum Übertragen der Datei auswählen.

Schritt 3. Installieren Sie den Administrationsagenten erneut auf Geräten, die durch Kaspersky Next Expert View verwaltet werden

Wenn Sie das autonome Installationspaket des Administrationsagenten erstellt haben, können Sie mit der Erstellung einer Aufgabe zur Remote-Installation fortfahren. Durch das Ausführen dieser Aufgabe können Sie den Administrationsagenten auf allen verwalteten Geräten erneut installieren, sodass diese Geräte unter die Verwaltung von Kaspersky Next Expert View gestellt werden.

Um das Risiko eines Datenverlusts zu verringern, empfehlen wir, die Vorgänge zunächst für eine kleine Administrationsgruppe auszuführen, die bis zu 20 verwaltete Geräte im Unternehmensnetzwerk besitzt und keine physischen Server enthält. Überprüfen Sie nach Abschluss dieser Vorgänge, ob die Neuinstallation erfolgreich abgeschlossen wurde, und setzen Sie die Neuinstallation für den vollständigen Installationsbereich fort.

So erstellen Sie eine Aufgabe zur Remote-Installation und installieren den Administrationsagenten erneut:

1. Kehren Sie zum Migrationsassistenten der lokal ausgeführten Kaspersky Security Center Web Console zurück.

   Wir empfehlen, den Migrationsassistenten zu verwenden, um eine Aufgabe zur Remote-Installation zu erstellen, mit welcher der Administrationsagent wie unten beschrieben neu installiert werden kann. Wenn es notwendig ist, eine benutzerdefinierte Aufgabe zur Remote-Installation zu verwenden, müssen Sie zunächst manuell ein benutzerdefiniertes Installationspaket aus dem autonomen Installationspaket des Administrationsagenten erstellen. Bitte beachten Sie, dass Sie beim Erstellen eines benutzerdefinierten Installationspakets in der Befehlszeile der ausführbaren Datei den Parameter "-s" angeben müssen. Andernfalls wird die Neuinstallation des Administrationsagenten aus diesem benutzerdefinierten Installationspaket mit einem Fehler abgeschlossen.

   Abhängig vom aktuellen Status des Migrationsassistenten können Sie einen der folgenden Schritte ausführen:

   - Wenn Sie den Migrationsassistenten nach dem Export nicht geschlossen haben und Ihre Sitzung nicht abgelaufen ist, klicken Sie auf die Schaltfläche **Weiter mit Schritt 3 des Migrationsassistenten**. Aktivieren Sie das Kontrollkästchen **Autonomes Installationspaket hochladen** und klicken Sie auf die Schaltfläche **Autonomes Installationspaket auswählen**. Geben Sie in dem sich öffnenden Browserfenster das autonome Installationspaket des Administrationsagenten an.

   - Falls Sie den Migrationsassistenten erneut starten müssen, aktivieren Sie das Kontrollkästchen **Autonomes Installationspaket hochladen** und klicken Sie auf die Schaltfläche **Autonomes Installationspaket auswählen**. Geben Sie in dem sich öffnenden Browserfenster das autonome Installationspaket des Administrationsagenten an. Danach zeigt der Migrationsassistent wieder die Hierarchie der Administrationsgruppen dieses Administrationsservers an. Wählen Sie dieselbe Gruppe aus, für die Sie die Exportdatei erstellt haben, und klicken Sie auf **Weiter**.

     Der Migrationsassistent überprüft erneut die Gesamtzahl der verwalteten Geräte, die in der ausgewählten Administrationsgruppe enthalten sind. Wenn diese Zahl 10.000 übersteigt, wird eine Fehlermeldung angezeigt. Die Schaltfläche **Weiter** bleibt solange inaktiv (ausgegraut), bis sich die Anzahl der verwalteten Geräte in der ausgewählten Administrationsgruppe innerhalb der Beschränkung befindet.

2. Warten Sie, bis das autonome Installationspaket hochgeladen wurde und klicken Sie auf **Weiter**. Der Migrationsassistent erstellt ein benutzerdefiniertes Installationspaket und eine Aufgabe zur Remote-Installation für dieses. Der Aufgabenbereich umfasst die Administrationsgruppe, die Sie in der Seite **Verwaltete Geräte für den Export** ausgewählt haben und der Zeitplan für den Start der Aufgabe wird standardmäßig auf **Manuell** gestellt. Der Migrationsassistent zeigt den Fortschritt der Erstellung an. Warten Sie, bis die Aktualisierungssymbole (↻) durch grüne Häkchen (✓) ersetzt wurden und klicken Sie auf **Weiter**.

3. Falls notwendig, aktivieren Sie das Kontrollkästchen **Neu erstellte Aufgabe zur Remote-Installation ausführen** (standardmäßig deaktiviert) für die Geräte in der ausgewählten Administrationsgruppe und alle ihrer Untergruppen des lokal ausgeführten Administrationsservers. In diesem Fall werden die Geräte unter Verwaltung von Kaspersky Next Expert View gestellt – jedoch erst nach Abschluss der Installation des Administrationsagenten. Es wird der vollständige Pfad zu der Administrationsgruppe angezeigt, in der die Aufgabe ausgeführt wird.

   Die Aufgabe darf erst gestartet werden, nachdem der Import in die Kaspersky Next Expert View abgeschlossen ist. Andernfalls werden die Gerätenamen möglicherweise in der Liste dupliziert.

4. Klicken Sie auf **Fertigstellen**, um den Migrationsassistenten zu schließen und starten Sie die Aufgabe zur Remote-Installation für folgende Zwecke:

   - Instanzen der Administrationsagenten aktualisieren
   - Instanzen der Administrationsagenten unter Verwaltung durch Kaspersky Next Expert View stellen

   Wenn Sie das Kontrollkästchen **Neu erstellte Aufgabe zur Remote-Installation ausführen** nicht aktiviert haben, können Sie die Aufgabe bei Bedarf später manuell starten.

Sie können jetzt überprüfen, ob Sie die migrierten Instanzen des Administrationsagenten über Kaspersky Next Expert View verwalten können. Wechseln Sie dazu nach **Asset-Verwaltung → Assets (Geräte)**. Stellen Sie sicher, dass für die migrierten verwalteten Geräte das Bestätigungssymbol (⊙) in den Spalten **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt** angezeigt wird. Stellen Sie außerdem sicher, dass diese Geräte nicht die Statusbeschreibung *Lange nicht verbunden* besitzen.

Migration mit Hierarchie von Administrationsservern

Dieser Abschnitt beschreibt die Migration von verwalteten Geräten und zugehörigen Objekten von einem lokal ausgeführten Kaspersky Security Center Web Console auf Kaspersky Next Expert View. Der Prozess umfasst eine Hierarchie: Die lokal ausgeführte Kaspersky Security Center Web Console fungiert als sekundärer Administrationsserver und Kaspersky Next Expert View fungiert als primärer Administrationsserver.

Jede Administrationsgruppe, die Sie an die Kaspersky Next Expert View übertragen, muss die verwalteten Geräte für jeweils ein Betriebssystem enthalten. Wenn in Ihrem Netzwerk Geräte mit verschiedenen Betriebssystemen enthalten sind, ordnen Sie diese verschiedenen Administrationsgruppen zu und migrieren Sie anschließend jede Gruppe separat.

Nach Abschluss der Migration sind alle Administrationsagenten in der Gruppe innerhalb des Migrationsbereichs aktualisiert und werden über Kaspersky Next Expert View verwaltet.

Erfüllen Sie zunächst die folgenden Voraussetzungen:

- Der lokal ausgeführte Administrationsserver wurde auf Version 14.2 oder höher aktualisiert.
- Installation von Kaspersky Security Center Web Console in Version 12.1 oder höher.
- Aktualisieren Sie die Administrationsagenten auf den verwalteten Geräten auf die Version 12 oder höher.
- Verwenden Sie auf Windows-Geräten den Administrationsagenten ohne Kennwort für die Deinstallation.

  Wenn das Kennwort bereits festgelegt wurde, führen Sie in der Kaspersky Security Center Web Console einen der folgenden Schritte aus:

  - Deaktivieren Sie die Option **Deinstallationskennwort verwenden** in den Richtlinieneinstellungen des Administrationsagenten.
  - Führen Sie unter Verwendung der Aufgabe *Remote-Deinstallation einer Anwendung* eine Remote-Deinstallation des Administrationsagenten durch. Wählen Sie im Feld **Zu deinstallierende Anwendung** der Aufgabe das Programm **Kaspersky Security Center Administrationsagent** aus. Vergessen Sie nicht, das Kennwort für die Deinstallation einzugeben.
- Aktualisieren Sie die verwalteten Programme auf Versionen, die von Kaspersky Next Expert View unterstützt werden.
- Stellen Sie sicher, dass Sie über Richtlinien für die neuesten Versionen des verwalteten Programms verfügen. Wenn Sie veraltete Richtlinien verwenden, erstellen Sie neue Richtlinien für die Versionen der Anwendung, die von Kaspersky Next Expert View unterstützt werden.
- Um aktuelle Richtlinien zu verwenden, aktualisieren Sie die Web-Plug-ins, für die Programme, die Sie durch Kaspersky Next Expert View verwalten möchten.
- Deinstallieren Kaspersky-Anwendungen von verwalteten Geräten, wenn diese Anwendungen nicht durch Kaspersky Next Expert View unterstützt werden.
- Entschlüsseln aller Daten (auf Festplatten- oder Dateiebene), die durch Kaspersky Endpoint Security für Windows auf verwalteten Windows-Geräten verschlüsselten wurden. Deaktivieren Sie anschließend auf den verwalteten Geräten die Verschlüsselungsfunktion entweder lokal oder über eine Anwendungsrichtlinie. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

  Befinden sich auf dem verwalteten Windows-Gerät immer noch Dateien oder Ordner, die von Kaspersky Endpoint Security für Windows verschlüsselt wurden, wird das Upgrade des Administrationsagenten während des Migrationsprozesses abgebrochen. Sie werden durch eine Meldung dazu aufgefordert, alle Daten auf dem Gerät zu entschlüsseln und die Verschlüsselungsfunktion zu deaktivieren.

Kaspersky Next Expert View unterstützt maximal 25.000 verwaltete Geräte pro Administrationsserver.

Um eine Migration auf Kaspersky Next Expert View durchzuführen:

1. Schätzen Sie den Umfang des Migrationsprozesses, d.h. die zu exportierende Administrationsgruppe, ein und bewerten Sie die Anzahl der darin verwalteten Geräte. Stellen Sie sicher, dass alle als Migrationsvoraussetzungen aufgeführten Aktivitäten erfolgreich abgeschlossen wurden.
2. Wechseln Sie in Kaspersky Next Expert View zum sekundären Administrationsserver der verwalteten Geräte, die Sie migrieren möchten.

3. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Migration**.

   Die Begrüßungsseite des Migrationsassistenten wird geöffnet.

4. Klicken Sie auf der Begrüßungsseite auf **Weiter**.

   Die Seite **Verwaltete Geräte für den Export** wird geöffnet und zeigt die gesamte Hierarchie der Administrationsgruppen des sekundären Administrationsservers an.

5. Klicken Sie auf der Seite **Verwaltete Geräte für den Export** auf das Chevron-Symbol (›) neben dem Gruppennamen **Verwaltete Geräte**, und erweitern Sie anschließend die Hierarchie der Administrationsgruppen. Wählen Sie die Administrationsgruppe aus, die Sie exportieren möchten.

   Der Migrationsassistent überprüft die Gesamtzahl der verwalteten Geräte, die in der ausgewählten Administrationsgruppe enthalten sind. Wenn diese Zahl 10.000 übersteigt, wird eine Fehlermeldung angezeigt. Die Schaltfläche **Weiter** bleibt solange inaktiv (ausgegraut), bis sich die Anzahl der verwalteten Geräte in der ausgewählten Administrationsgruppe innerhalb der Beschränkung befindet.

6. Wählen Sie die verwalteten Programme aus, deren Richtlinien und Aufgaben zusammen mit Gruppenobjekten an Kaspersky Next Expert View übertragen werden müssen. Um die verwalteten Programme auszuwählen, deren Objekte exportiert werden sollen, aktivieren Sie die Kontrollkästchen neben ihren Namen in der Liste.

   Der Kaspersky Security Center Administrationsserver wird zwar in der Liste aufgeführt, allerdings erfolgt bei entsprechend aktiviertem Kontrollkästchen kein Export von dessen Richtlinien.

   Um sicherzugehen, dass Ihre verwalteten Programme von Kaspersky Next Expert View unterstützt werden, klicken Sie auf den entsprechenden Link. Dieser öffnet in der Online-Hilfe einen Abschnitt mit einer Liste verwalteter Programme, die von Kaspersky Next Expert View unterstützt werden.

   Wenn Sie Programme auswählen, die von der Kaspersky Next Expert View nicht unterstützt werden, so werden die Richtlinien und Aufgaben dieser Programme trotzdem migriert. Diese können jedoch aufgrund fehlender dezidierter Plug-ins nicht in Kaspersky Next Expert View verwaltet werden.

7. Die Liste der standardmäßig exportierten Gruppenobjekte anzeigen. Bei Bedarf können Sie auch Objekte ohne Gruppenzugehörigkeit angeben, die zusammen mit der ausgewählten Administrationsgruppe exportiert werden sollen, beispielsweise: globale Aufgaben, benutzerdefinierte Geräteauswahlen, Berichte, benutzerdefinierte Rollen, interne Benutzer und Sicherheitsgruppen sowie benutzerdefinierte Programmkategorien mit manuell hinzugefügtem Inhalt. Diese Seite enthält die folgenden Abschnitte:

   - **Globale Aufgaben**

     Die Liste mit den globalen Aufgaben der verwalteten Anwendungen sowie der globalen Aufgaben des Administrationsagenten.

     Wenn eine von Ihnen ausgewählte globale Aufgabe für eine bestimmte Objektauswahl gilt, wird diese Auswahl ebenfalls exportiert.

     Die globalen Aufgaben des Administrationsservers werden zwar in der Liste aufgeführt, allerdings können sie nicht exportiert werden. Wenn Sie diese Aufgaben auswählen, ändert sich der Exportbereich nicht. Es werden außerdem keine Aufgaben zur Remote-Installation in den Exportbereich aufgenommen, da deren zugehörigen Installationspakete nicht exportiert werden können.

- **Geräteauswahlen**

  Die Liste mit benutzerdefinierten Geräteauswahlen.

- **Berichte**

  Die bearbeitbare Liste mit zu exportierenden Instanzen der Berichte.

  > Wenn ein von Ihnen ausgewählter Bericht für eine bestimmte Objektauswahl gilt, wird diese Auswahl ebenfalls exportiert.

  > Da Kaspersky Next Expert View die gleichen Berichtsvorlagen wie Kaspersky Security Center Web Console enthält, können Sie nur die Berichte für den Export auswählen, die Sie manuell erstellt oder konfiguriert haben.

- **Gruppenobjekte**

  Die Liste der standardmäßig exportierten Gruppenobjekte. Die folgenden Objekte, die sich auf die ausgewählte Administrationsgruppe beziehen, werden standardmäßig vollständig exportiert:

  - Struktur der Administrationsgruppen, d. h. alle untergeordneten Gruppen der ausgewählten Administrationsgruppe.
  - Geräte, die in den zu exportierenden Administrationsgruppen enthalten sind.
  - Tags, die den zu exportierenden Geräten zugewiesen wurden.

    > Wenn ein Tag in Kaspersky Security Center Web Console erstellt, aber keinem Gerät zugewiesen wurde, wird es nicht exportiert. Die Regeln für die automatische Tag-Zuweisung werden ebenfalls nicht exportiert.

  - Gruppenrichtlinien der ausgewählten verwalteten Anwendungen.

    > Richtlinien des Administrationsservers und des Administrationsagenten werden nicht exportiert.

  - Gruppenaufgaben der ausgewählten verwalteten Anwendungen und des Administrationsagenten.

    > Aufgaben des Administrationsservers werden nicht exportiert.

  Sie können das Exportieren bestimmter Arten von Nicht-Gruppenobjekten auch verhindern:

  - Um den Export benutzerdefinierter Rollen (d.h. nur diejenigen, die vom Benutzer erstellt wurden) abzubrechen, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Rollen vom Export ausschließen**.
  - Um den Export interner Benutzer und Sicherheitsgruppen abzubrechen, aktivieren Sie das Kontrollkästchen **Interne Benutzer und Sicherheitsgruppen vom Export ausschließen**.
  - Um den Export benutzerdefinierter Programmkategorien mit manuell hinzugefügtem Inhalt abzubrechen, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Programmkategorien vom Export ausschließen**.

Wenn Sie Geräte mit verschiedenen Betriebssystemen in die Kaspersky Next Expert View übertragen, müssen Objekte, die keiner Gruppe entsprechen, nur einmal migriert werden.

8. Nachdem Sie den Migrationsbereich definiert haben, klicken Sie auf **Weiter**, um den Exportvorgang zu starten. Die Seite **Exportdatei wird erstellt** wird geöffnet, auf der Sie den Exportfortschritt aller Objekttypen anzeigen können, die Sie in den Migrationsbereich aufgenommen haben. Warten Sie, bis jedes Aktualisierungssymbol (🔄) neben jedem Element in der Objektliste durch ein grünes Häkchen (✓) ersetzt wurde. Der Export wird beendet und die Exportdatei wird automatisch in einem temporären Ordner gespeichert. Die nächste Seite wird geöffnet und zeigt die gesamte Hierarchie der Administrationsgruppen in Kaspersky Next Expert View an, das als primärer Administrationsserver fungiert.

9. Aktivieren Sie das Kontrollkästchen neben der Administrationsgruppe, in welche die Gruppenobjekte importiert werden sollen und klicken Sie anschließend auf **Weiter**. Die Datei wird entpackt und die Nicht-Gruppenobjekte und Gruppenobjekte werden in der Ziel-Administrationsgruppe wiederhergestellt.

   Wenn der Name des wiederherzustellenden Objekts mit dem Namen eines bereits vorhandenen Objekts identisch ist, besitzt das wiederhergestellte Objekt ein inkrementelles Suffix.

   Nach Abschluss des Imports wird die exportierte Struktur der Administrationsgruppen einschließlich der Gerätedetails unter der von Ihnen ausgewählten Ziel-Administrationsgruppe angezeigt. Die Nicht-Gruppenobjekte werden ebenfalls importiert.

   Sie können den Migrationsassistenten während des Imports nicht minimieren und keine gleichzeitigen Vorgänge ausführen. Warten Sie, bis jedes Aktualisierungssymbol (🔄) neben jedem Element in der Objektliste durch ein grünes Häkchen (✓) ersetzt wurde und der Import beendet ist. Anschließend beginnen die Geräte mit dem Wechsel zu Kaspersky Next Expert View.

10. Nach Abschluss des Imports zeigt der Migrationsassistent eine Liste der Installationspakete des Administrationsagenten an, die in Kaspersky Next Expert View für ein entsprechendes Betriebssystem verfügbar sind. Wählen Sie das Installationspaket mit der entsprechenden Version und Lokalisierung des Administrationsagenten aus.

    Wählen Sie das Installationspaket des Administrationsagenten für Windows nur aus, wenn Sie zuvor in Ihrem Arbeitsbereich von Kaspersky Next Expert View den Schnellstartassistenten abgeschlossen und die Migration der Windows-Geräte durchgeführt haben.

11. Klicken Sie auf die Schaltfläche **Weiter**.

    Der Migrationsassistent erstellt ein neues autonomes Installationspaket (oder verwendet ein vorhandenes) und ein darauf basierendes benutzerdefiniertes Installationspaket sowie die entsprechende Aufgabe zur Remote-Installation. Der Aufgabenbereich beinhaltet die Administrationsgruppe, die Sie auf der Seite **Verwaltete Geräte für den Export** ausgewählt haben. Der Zeitplan für den Start der Aufgabe ist standardmäßig auf **Manuell** eingestellt. Der Migrationsassistent zeigt den Fortschritt der Erstellung an.

12. Warten Sie, bis jedes Aktualisierungssymbol (🔄) durch ein grünes Häkchen (✓) ersetzt wurde und klicken Sie auf **Weiter**.

13. Falls notwendig, aktivieren Sie das Kontrollkästchen **Neu erstellte Aufgabe zur Remote-Installation ausführen** (standardmäßig deaktiviert) für die Geräte in der ausgewählten Administrationsgruppe in der lokal ausgeführten Kaspersky Security Center Web Console, sowie all ihrer Untergruppen. Nach Abschluss der Installation des Administrationsagenten können Sie die ausgewählten Geräte über die Kaspersky Next Expert View verwalten. Es wird der vollständige Pfad zu der Administrationsgruppe angezeigt, in welcher die Aufgabe ausgeführt wird.

    Die Aufgabe zur Remote-Installation darf erst gestartet werden, nachdem der Import in die Kaspersky Next Expert View abgeschlossen ist. Andernfalls kann es passieren, dass die Geräte dupliziert werden.

14. Klicken Sie auf **Fertigstellen**, um den Migrationsassistenten zu schließen und starten Sie die Aufgabe zur Remote-Installation für folgende Zwecke:

    - Instanzen der Administrationsagenten aktualisieren
    - Instanzen der Administrationsagenten durch Kaspersky Next Expert View verwalten

    Wenn Sie das Kontrollkästchen **Aufgabe zur Remote-Installation ausführen** nicht aktiviert haben, können Sie die Aufgabe bei Bedarf später manuell starten.

Sie können jetzt überprüfen, ob Sie die migrierten Instanzen des Administrationsagenten über Kaspersky Next Expert View verwalten können. Wechseln Sie dazu nach **Asset-Verwaltung** → **Assets (Geräte)**. Stellen Sie sicher, dass für die migrierten verwalteten Geräte das Bestätigungssymbol (✓) in den Spalten **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt** angezeigt wird. Stellen Sie außerdem sicher, dass diese Geräte nicht die Statusbeschreibung *Lange nicht verbunden* besitzen.

Szenario: Migration von Geräten mit Linux- oder macOS-Betriebssystem

Dieser Abschnitt beschreibt die Migration von Geräten mit Linux- oder macOS-Betriebssystem von einer lokal ausgeführten Kaspersky Security Center Web Console auf Kaspersky Next Expert View. Die grundlegenden Szenarien der Migration ohne Hierarchie von Administrationsservern und der Migration mit einer solchen Hierarchie erlauben Ihnen die Übertragung aller Geräte und zugehöriger Objekte an die Kaspersky Next Expert View. Wenn Ihr Netzwerk jedoch Geräte umfasst, auf denen nicht nur Windows, sondern auch Linux oder macOS ausgeführt wird, müssen Sie die Geräte für jede Art von Betriebssystem separat übertragen. Sie müssen daher die Migration mehrmals durchführen.

Erforderliche Vorrausetzungen

Führen Sie vor dem Start Folgendes durch:

- Aktualisieren Sie den lokal ausgeführten Administrationsserver auf Version 12 Patch A oder höher aktualisiert.
- Installieren Sie die Kaspersky Security Center Web Console in Version 12.1 oder höher.
- Aktualisieren Sie die Administrationsagenten auf den verwalteten Geräten auf die Version 12 oder höher.

- Aktualisieren Sie die verwalteten Programme auf Versionen, die von Kaspersky Next Expert View unterstützt werden.
- Stellen Sie sicher, dass Sie über Richtlinien für die neuesten Versionen des verwalteten Programms verfügen. Wenn Sie veraltete Richtlinien verwenden, erstellen Sie neue Richtlinien für die Versionen der Anwendung, die von Kaspersky Next Expert View unterstützt werden.
- Um aktuelle Richtlinien zu verwenden, aktualisieren Sie die Web-Plug-ins, für die Programme, die Sie durch Kaspersky Next Expert View verwalten möchten.
- Deinstallieren Sie Kaspersky-Anwendungen, die nicht von Kaspersky Next Expert View unterstützt werden, von den verwalteten Geräten und ersetzen Sie anschließend die deinstallierten Anwendungen durch unterstützte.

Kaspersky Next Expert View unterstützt maximal 25.000 verwaltete Geräte pro Administrationsserver.

Schritte der Migration

Die Migration auf Kaspersky Next Expert View umfasst die folgenden Schritte:

1. **Verwaltete Geräte entsprechend ihren Betriebssystemen gruppieren**

   Wenn in Ihrem Netzwerk Geräte mit unterschiedlichen Betriebssystemen enthalten sind (Windows, Linux oder macOS), platzieren Sie die Geräte in der Kaspersky Security Center Web Console für jedes Betriebssystems in separaten Administrationsgruppen. Erstellen Sie dabei eine Administrationsgruppe für jede Linux-Distribution. Wenn Sie beispielsweise über verschiedene Linux-Geräte mit Debian und mit Red Hat verfügen, weisen Sie diesen verschiedene Administrationsgruppen zu. Auf diese Weise können Sie die Migration erfolgreich durchführen, da für verschiedene Betriebssysteme unterschiedliche Installationspakete des Administrationsagenten erforderlich sind.

2. **Die Migration jeder Administrationsgruppe und ihrer Programmobjekte separat durchführen**

   Die verwalteten Geräte eines jeden Betriebssystems müssen separat migriert werden, um ihre Richtlinien und Aufgaben einzuschließen. Wenn Sie beispielsweise über verschiedene Geräte mit Windows, macOS, Ubuntu und CentOS verfügen, übertragen Sie zuerst die Windows-Geräte auf die Kaspersky Next Expert View, anschließend die macOS-Geräte, dann die Ubuntu-Geräte und letztlich die CentOS-Geräte. Sie können die verwalteten Geräte in beliebiger Reihenfolge übertragen.

   Führen Sie dazu, in Abhängigkeit davon, ob Ihr Netzwerk sekundäre Administrationsserver enthält, entweder die Migration ohne Hierarchie der Administrationsserver oder die Migration mit einer solchen Hierarchie durch. Verwenden Sie während der Migration das Installationspaket des Administrationsagenten, das dem Betriebssystem der übertragenen Geräte entspricht. Wählen Sie beispielsweise den Kaspersky Security Center 13.2 Administrationsagenten für Linux-Geräte aus, um deren Migration erfolgreich durchzuführen.

   Beachten Sie, dass Objekte, die keiner Gruppe entsprechen, wie globale Aufgaben, benutzerdefinierte Geräteauswahlen oder Berichte, nur einmal migriert werden.

Ergebnisse

Nach dem Abschluss der Migration kann durch folgende Punkte sichergestellt werden, dass diese erfolgreich verlaufen ist:

- Auf jedem verwalteten Linux- oder macOS-Gerät ist die passende Version des Administrationsagenten neu installiert.
- Alle Linux- oder macOS-Geräte werden durch Kaspersky Next Expert View verwaltet.
- Alle Objekteinstellungen, die vor der Migration wirksam waren, sind erhalten geblieben.

Szenario: Rückmigration von Kaspersky Next Expert View auf Kaspersky Security Center

Unter Umständen kann die Migration von verwalteten Geräten aus Kaspersky Next Expert View auf Kaspersky Security Center Administrationsserver notwendig werden. Sie können dieses Szenario beispielsweise für ein Rollback der Migration auf Kaspersky Next Expert View verwenden.

Erforderliche Vorrausetzungen

Stellen Sie vor dem Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Kaspersky Next Expert View ist verfügbar und es sind verwaltete Geräte mit ihm verbunden.
- Der Kaspersky Security Center 14.2 (oder höher) Administrationsserver ist verfügbar und besitzt ein Installationspaket des Administrationsagenten ab Version 13.

Schritte der Rückmigration

Die Rückmigration umfasst die folgenden Schritte:

1. **Erstellen eines autonomen Installationspakets des Administrationsagenten im lokal ausgeführten Kaspersky Security Center Administrationsserver**

   Erstellen Sie ein autonomes Installationspaket des Administrationsagenten im lokal ausgeführten Kaspersky Security Center Administrationsserver.

   Im Laufe der Erstellung können Sie die Option **Nicht zugeordnete Geräte in folgende Gruppe verschieben** auswählen, um eine Administrationsgruppe anzugeben, in welche die Administrationsagenten nach der Installation verschoben werden sollen. Wenn Sie eine Administrationsgruppe angegeben haben, wird eine automatische Verschiebungsregel erstellt, die alle mit diesem autonomen Installationspaket installierten Administrationsagenten in die Ziel-Administrationsgruppe verschiebt.

Um eine fehlerfreie Rückmigration zu gewährleisten, stellen Sie sicher, dass Sie für den Administrationsagenten eine Version auswählen, die dem verwendeten Administrationsagenten von Kaspersky Next Expert View entweder entspricht oder aktueller ist.

2. **Erstellen eines benutzerdefinierten Installationspakets in Kaspersky Next Expert View**

   Wechseln Sie zu Kaspersky Next Expert View und erstellen Sie ein benutzerdefiniertes Installationspaket auf Grundlage des autonomen Installationspakets, dass Sie in dem lokal ausgeführten Kaspersky Security Center Administrationsserver erstellt und gespeichert haben.

   Um die Paketinstallation im Silent-Modus zu aktivieren, geben Sie im Feld **Kommandozeilenparameter der ausführbaren Datei** den Parameter `-s` an.

3. **Erstellen einer Aufgabe zur Remote-Installation**

   Erstellen Sie in Kaspersky Next Expert View eine Aufgabe zur Remote-Installation. Verwenden Sie dazu das benutzerdefinierte Installationspaket, das Sie erstellt haben.

4. **Starten der Aufgabe zur Remote-Installation**

   Starten Sie die von Ihnen erstellte Aufgabe zur Remote-Installation. Die Aufgabe führt die Neuinstallation aller in der Administrationsgruppe angegeben Administrationsagenten durch, und stellt diese durch Anpassen der Verbindungsadresse und anderer Verbindungseinstellungen unter Verwaltung des lokal ausgeführten Kaspersky Security Center Administrationsservers.

   Wenn Sie bei der Erstellung des autonomen Installationspakets keine Ziel-Administrationsgruppe angegeben haben, werden alle Geräte in die Gruppe **Nicht zugeordnete Geräte** verschoben.

Ergebnisse

Nach dem Abschluss der Migration kann durch folgende Punkte sichergestellt werden, dass diese erfolgreich verlaufen ist:

- Alle Geräte, die in den Bereich der Aufgabe zur Remote-Installation fallen und die ursprünglich durch Kaspersky Next Expert View verwaltet wurden, werden jetzt durch den lokal ausgeführten Kaspersky Security Center Administrationsserver verwaltet.
- Die Geräte wurden automatisch in die Administrationsgruppe verschoben, die in den Einstellungen des Installationspakets angegeben wurde.

Die Aufgabe zur Remote-Installation kann in Kaspersky Next Expert View nicht abgeschlossen werden: Die Aufgabe besitzt keine Zielgeräte mehr, da sich für diese die Verbindungseinstellungen geändert haben. Sie müssen die Aufgabe manuell beenden, nachdem Sie sichergestellt haben, dass für alle Geräte, die sich im Migrationsbereich befinden, in der Spalte **Sichtbar** der Liste mit verwalteten Geräten das Fehler-Icon (!) angezeigt wird.

Migration mit virtuellen Administrationsservern

Wenn Sie in Ihrer lokalen Infrastruktur von Kaspersky Security Center virtuelle Administrationsserver besitzen, können Sie die Migration von dem lokalen Kaspersky Security Center auf Kaspersky Next Expert View nicht mit Migrationsassistenten durchführen. Zudem können Sie nur die Geräte Ihrer Kunden migrieren. Sie müssen Richtlinien, Aufgaben und Berichte manuell erstellen.

Sie können eine Migration mittels einem der folgenden Szenarien durchführen:

- Durch verschieben Ihrer Kundengeräte von einem virtuellen Administrationsserver auf einen primären Administrationsserver
- Durch manuelle Migration aus den virtuellen Administrationsservern

Szenario: Migration mit virtuellen Administrationsservern und durch Verschieben von Geräten

Um die Migration von einer lokal ausgeführten Kaspersky Security Center Web Console zur Kaspersky Next Expert View durchzuführen, können Sie Ihre Geräte von virtuellen Administrationsservern auf einen primären Administrationsserver verschieben.

Erforderliche Vorrausetzungen

Vor dem Beginn der Migration müssen Sie eine Reihe von Aktionen ausführen, einschließlich der Aktualisierung des lokal ausgeführten Administrationsservers auf Version 12 oder höher und der Aktualisierung der verwalteten Programme auf Versionen, die durch Kaspersky Next Expert View unterstützt werden.

Migrationsszenario

Das Szenario verläuft in den folgenden Schritten:

1. **Anlegen einer Administrationsgruppe für jeden Ihrer virtuellen Administrationsserver**

   Das Erstellen der Gruppe findet in Ihrem lokal ausgeführten Kaspersky Security Center statt.

2. **Verschieben Ihrer Kundengeräte**

   Wechseln Sie in das lokal ausgeführte Kaspersky Security Center und verschieben Sie die Geräte Ihrer Kunden aus jedem virtuellen Administrationsserver in die im vorherigen Schritt angelegte entsprechende Administrationsgruppe.

3. **Migration**

   Führen Sie die Migration durch, wie für eine Netzwerk ohne Hierarchie von Administrationsservern beschrieben.

4. **Geräte unter die Verwaltung virtueller Administrationsserver verschieben (optionaler Schritt)**

   Wenn Sie Ihre Kunden mittels virtuellen Administrationsservern verwalten möchten, verschieben Sie die Geräte aus den Administrationsgruppen unter der Verwaltung von virtuellen Administrationsservern.

5. **Erstellen Sie Richtlinien, Aufgaben und Berichte**

   Erstellen Sie benötigte Richtlinien, Aufgaben und Berichte.

Ergebnisse

Nach dem Abschluss der Migration kann durch folgende Punkte sichergestellt werden, dass diese erfolgreich verlaufen ist:

- Der Administrationsagent wurde auf allen verwalteten Geräten neu installiert.
- Alle Geräte werden durch Kaspersky Next Expert View verwaltet.
- Alle Objekteinstellungen, die vor der Migration wirksam waren, sind erhalten geblieben.

Szenario: Manuelle Migration mit virtuellen Administrationsservern

Sie können von einer lokal ausgeführten Kaspersky Security Center Web Console zur Kaspersky Next Expert View manuell migrieren.

Erforderliche Vorrausetzungen

Vor dem Beginn der Migration müssen Sie eine Reihe von Aktionen ausführen, einschließlich der Aktualisierung des lokal ausgeführten Administrationsservers auf Version 12 oder höher und der Aktualisierung der verwalteten Programme auf Versionen, die durch Kaspersky Next Expert View unterstützt werden.

Migrationsszenario

Das Szenario verläuft in den folgenden Schritten:

1. **Anlegen einer Administrationsgruppe für jeden Ihrer virtuellen Administrationsserver**

   Wechseln Sie zu Kaspersky Next Expert View und legen Sie eine Administrationsgruppe an, die jedem Ihrer virtuellen Administrationsserver entspricht.

2. **Ein autonomes Installationspaket für den Administrationsagenten erstellen**

   Erstellen eines autonomen Installationspakets für den Administrationsagenten. Geben Sie während der Erstellung die Administrationsgruppe an, die Sie im vorhergehenden Schritt angelegt haben. Dies bedeutet, dass Sie für jede Administrationsgruppe ein individuelles autonomes Installationspaket erstellen müssen.

   Dieser Schritt findet in Ihrer Kaspersky Next Expert View statt.

3. **Herunterladen der autonomen Installationspakete**

   Laden Sie das autonome Installationspaket herunter, welches Sie im vorhergehenden Schritt erstellt haben. Dieser Schritt findet in Ihrer Kaspersky Next Expert View statt.

4. **Anlegen eines Archivs für jedes autonome Installationspaket**

   Die folgenden Archivtypen werden unterstützt: ZIP, CAB, TAR oder TAR.GZ.

5. **Erstellen von benutzerdefinierten Installationspaketen für den Administrationsagenten**

   Erstellen Sie benutzerdefinierte Installationspakete für den Administrationsagenten. Wählen Sie während der Erstellung die Archive aus, die Sie im vorhergehenden Schritt angelegt haben.

   Dieser Schritt findet in Ihrem lokal ausgeführten Kaspersky Security Center statt.

6. **Erstellen von Aufgaben zur Remote-Installation**

   Legen Sie Aufgaben zur Remote-Installation an, um den aus den benutzerdefinierten Installationspaketen erstellten Administrationsagent zu installieren.

   Geben Sie bei der Erstellung jeder Aufgabe die entsprechende Administrationsgruppe an.

   Dieser Schritt findet in Ihrem lokal ausgeführten Kaspersky Security Center statt.

7. **Starten der erstellten Aufgaben zur Remote-Installation**

   Die Administrationsagenten werden aktualisiert. Der Administrationsserver von Kaspersky Next Expert View übernimmt deren Verwaltung.

   Alle Geräte werden nach Kaspersky Next Expert View migriert und in der Administrationsgruppe platziert, die Sie während der Erstellung des autonomen Installationspakets des Administrationsagenten angegeben haben.

8. **Geräte unter die Verwaltung virtueller Administrationsserver verschieben (optionaler Schritt)**

   Wenn Sie Ihre Kunden mittels virtuellen Administrationsservern verwalten möchten, verschieben Sie die Geräte aus den Administrationsgruppen unter der Verwaltung von virtuellen Administrationsservern.

9. **Erstellen Sie Richtlinien, Aufgaben und Berichte**

   Erstellen Sie benötigte Richtlinien, Aufgaben und Berichte.

Ergebnisse

Nach dem Abschluss der Migration kann durch folgende Punkte sichergestellt werden, dass diese erfolgreich verlaufen ist:

- Der Administrationsagent wurde auf allen verwalteten Geräten neu installiert.
- Alle Geräte werden durch Kaspersky Next Expert View verwaltet.

  Alle Objekteinstellungen, die vor der Migration wirksam waren, sind erhalten geblieben.

Szenario: Geräte aus Administrationsgruppen unter die Verwaltung von virtuellen Servern verschieben

Es kann vorkommen, dass Sie Ihre Kunden über virtuelle Administrationsserver verwalten wollen. Wenn Sie Geräte und andere Objekte von einem lokalen Kaspersky Security Center in die Kaspersky Next Expert View migriert haben, befinden sich die Geräte in Administrationsgruppen. Um die Geräte der Kunden über virtuelle Administrationsserver zu verwalten, müssen Sie die Geräte aus den Administrationsgruppen unter die Verwaltung virtueller Administrationsserver stellen.

Erforderliche Vorrausetzungen

Sie haben für jeden Ihrer Kunden einen virtuellen Administrationsserver erstellt.

Alle Geräte eines jeden Kunden befinden sich in einer individuellen Administrationsgruppe.

Schritte

Das Szenario verläuft in den folgenden Schritten:

1. **Ein autonomes Installationspaket für den Administrationsagenten erstellen**

   Wechseln Sie zu jedem der erstellten virtuellen Administrationsserver, und erstellen Sie ein eigenständiges Installationspaket für den Administrationsagenten. Sie können die Administrationsserver im Hauptmenü wechseln, indem Sie auf das Chevron-Symbol (›) rechts neben dem Namen des aktuellen Administrationsservers klicken und anschließend den benötigten Administrationsserver auswählen.

2. **Herunterladen der autonomen Installationspakete**

   Laden Sie das autonome Installationspaket herunter, welches Sie im vorhergehenden Schritt erstellt haben.

3. **Anlegen eines Archivs für jedes autonome Installationspaket**

   Die folgenden Archivtypen werden unterstützt:.zip, .cab, .tar und .tar.gz.

4. **Erstellen von benutzerdefinierten Installationspaketen für den Administrationsagenten**

   Erstellen Sie benutzerdefinierte Installationspakete für den Administrationsagenten. Wählen Sie während der Erstellung die Archive aus, die Sie im vorhergehenden Schritt angelegt haben.

   Dieser Schritt findet auf dem primären Administrationsserver statt.

5. **Erstellen von Aufgaben zur Remote-Installation**

   Legen Sie Aufgaben zur Remote-Installation an, um den aus den benutzerdefinierten Installationspaketen erstellten Administrationsagent zu installieren.

   Geben Sie bei der Erstellung jeder Aufgabe die entsprechende Administrationsgruppe an.

   Dieser Schritt findet auf dem primären Administrationsserver statt.

6. **Starten der erstellten Aufgaben zur Remote-Installation**

   Die Administrationsagenten werden aktualisiert. Die Geräte werden unter Verwaltung durch virtuelle Administrationsserver gesetzt.

7. **Erstellen Sie Richtlinien, Aufgaben und Berichte**

   Erstellen Sie benötigte Richtlinien, Aufgaben und Berichte.

Ergebnisse

Sie können jetzt die migrierten Kundengeräte mittels virtueller Administrationsserver verwalten.

Schnellstartassistent

In diesem Abschnitt finden Sie Informationen über den Schnellstartassistenten für Kaspersky Next Expert View.

Über den Schnellstartassistenten

Mit dem Schnellstartassistenten von Kaspersky Next Expert View können Sie die minimal erforderlichen Aufgaben und Richtlinien erstellen, eine Mindestauswahl an Einstellungen anpassen und mit dem Erstellen von Installationspaketen für Kaspersky-Anwendungen beginnen. Im Assistenten können Sie die folgenden Änderungen an Kaspersky Next Expert View vornehmen:

- Das Herunterladen von Installationspaketen für verwaltete Kaspersky-Anwendungen initiieren.
- Ein autonomes Installationspaket des Administrationsagenten erstellen, welches für Geräte mit Windows, Linux oder macOS vorgesehen ist.
- Erstellen der Richtlinie für den Kaspersky Security Center Administrationsagenten.
- Erstellen der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*.
- Erstellen Sie Richtlinien und Aufgaben für verwaltete Kaspersky-Anwendungen.
- Interaktion mit Kaspersky Security Network (KSN) konfigurieren.

Nachdem der Schnellstartassistent abgeschlossen wurde, werden die Installationspakete für den Administrationsagenten und für verwaltete Kaspersky-Anwendungen in der Liste **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete** angezeigt.

Der Schnellstartassistent erstellt Richtlinien für verwaltete Anwendungen, wie beispielsweise Kaspersky Endpoint Security für Windows, es sei denn, diese Richtlinien werden 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 Next Expert View fordert Sie automatisch zur Ausführung des Schnellstartassistenten auf, nachdem Sie einen Unternehmensarbeitsbereich erstellt und Kaspersky Next Expert View zum ersten Mal gestartet haben. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

Den Schnellstartassistent ausführen

Kaspersky Next Expert View fordert Sie automatisch zur Ausführung des Schnellstartassistenten auf, nachdem Sie einen Unternehmensarbeitsbereich erstellt und Kaspersky Next Expert View zum ersten Mal gestartet haben. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

Wenn Sie den Schnellstartassistenten erneut ausführen, werden die Aufgaben und Richtlinien, die bei der vorherigen Ausführung des Assistenten erstellt wurden, nicht neu erstellt.

So starten Sie den Schnellstartassistenten manuell:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Allgemein** aus.

3. Klicken Sie auf die Schaltfläche **Schnellstartassistent starten**.

   Alternativ können Sie den Schnellstartassistenten durch auswählen von **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Schnellstartassistent** starten.

Der Assistent fordert Sie auf, die Erstkonfiguration von Kaspersky Next Expert View durchzuführen. Folgen Sie den Schritten des Assistenten. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort. Verwenden Sie die Schaltfläche **Zurück**, um zum vorherigen Schritt des Assistenten zurückzukehren.

Schritt 1. Auswählen der herunterzuladenden Installationspakete

Wählen Sie die auf den Client-Geräten zu installierenden Kaspersky-Anwendungen aus der Liste aus. Für die ausgewählten Programme erstellt Kaspersky Next Expert View Installationspakete. Sie werden die erstellten Installationspakete später verwenden, um die Programme zu installieren.

Wenn Sie ein Installationspaket für den Download auswählen, beachten Sie die Sprache: Installationspakete stehen in verschiedenen Sprachen bereit.

Wählen Sie folgenden Programme aus:

- Kaspersky Security Center Administrationsagent

  Beachten Sie bei der Auswahl der Installationspakete des Administrationsagenten folgendes:

  - Der Administrationsagent muss auf jedem Client-Gerät installiert werden. Es ist deshalb notwendig, für jedes auf den Client-Geräten ausgeführte Betriebssystem einen passenden Administrationsagenten auszuwählen.

  - Der Administrationsagent muss durch ein autonomes Installationspaket manuell auf einem Gerät installiert werden, welches nach Ihrer Einschätzung als Verteilungspunkt fungieren soll. Verteilungspunkte müssen Netzwerkabfragen und Remote-Installation von Kaspersky-Sicherheitsanwendungen auf Client-Geräten durchführen können. Sie müssen daher mindestens ein Installationspaket des Administrationsagenten auswählen. Während Sie mit dem nächsten Schritt des Assistenten fortfahren, erstellt Kaspersky Next Expert View das autonome Installationspaket des Administrationsagenten.

    Im Vergleich mit Windows-basierten Verteilungspunkten, verfügen Linux- und macOS-basierte Verteilungspunkte über einen eingeschränkten Funktionsmodus. Es wird daher dringend empfohlen, dass Sie Windows-basierte Computer auswählen, die als Verteilungspunkte fungieren sollen.

Sie können Administrationsagenten für Windows, Linux und macOS auswählen. Wenn Sie den Administrationsagenten nur für ein Betriebssystem auswählen, z. B. für macOS, wird für das ausgewählte Betriebssystem ein autonomes Installationspaket erstellt. Wenn Sie den Administrationsagenten für mehrere Betriebssysteme auswählen, erstellt Kaspersky Next Expert View nur ein autonomes Installationspaket entsprechend der folgenden Prioritäten: Windows besitzt die höchste Priorität, gefolgt von Linux und anschließend macOS. Wenn Sie beispielsweise die Administrationsagenten für Linux und macOS ausgewählt haben, erstellt Kaspersky Next Expert View ein autonomes Installationspaket des Administrationsagenten für Linux. Sie können jederzeit manuell ein autonomes Installationspaket des Administrationsagenten für jedes dieser Betriebssysteme erstellen.

- Kaspersky-Sicherheitsanwendungen

  Wählen Sie Installationspakete, die für die auf den Client-Geräten in Ihrem Unternehmen installierten Betriebssysteme geeignet sind.

Schritt 2. Konfigurieren eines Proxyservers

Wenn Ihre Organisation einen Proxyserver verwendet, um eine Verbindung zum Internet herzustellen, geben Sie in diesem Schritt des Assistenten die Einstellungen des Proxyservers an. Diese Einstellungen werden dem Installationspaket des Administrationsagenten hinzugefügt. Nach der Installation wendet der Administrationsagent diese Einstellungen automatisch auf jedem Client-Gerät an.

Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

- **Proxyserver verwenden**
- **Adresse**
- **Port**
- **Authentifizierung am Proxyserver**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern 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.

- **Benutzername**

  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.

Schritt 3. Kaspersky Security Network konfigurieren

Wenn Sie im ersten Schritt des Assistenten das Installationspaket für Kaspersky Endpoint Security für Windows heruntergeladen haben, wird der Text der KSN-Erklärung für die folgenden Programme angezeigt:

- Kaspersky Endpoint Security für Windows
- Auf lokalen Geräten installiertes Kaspersky Security Center
- In einer Cloud-Umgebung installierte Kaspersky Next Expert View

Wenn Sie das Installationspaket von Kaspersky Endpoint Security für Windows nicht heruntergeladen haben, wird die KSN-Erklärung für dieses Programm nicht angezeigt.

Im Testmodus wird nur die KSN-Erklärung für Kaspersky Endpoint Security für Windows angezeigt.

Lesen Sie sich die Erklärung zu Kaspersky Security Network sorgfältig durch. Wählen Sie eine der folgenden Varianten aus:

- **Ich stimme der Teilnahme an Kaspersky Security Network zu**

  Kaspersky Next Expert View und die verwalteten Programme, die auf Client-Geräten installiert sind, übertragen ihre Betriebsdetails 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 Teilnahme an Kaspersky Security Network ab**

  Kaspersky Next Expert View und verwaltete Programme senden keine Informationen an Kaspersky Security Network.

  Wenn Sie diese Option auswählen, wird die Verwendung von Kaspersky Security Network deaktiviert.

Diese Verwendung von KSN ist standardmäßig deaktiviert. Wenn Sie Ihre Meinung zur Verwendung von KSN später ändern, können Sie die entsprechende Option im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN-Einstellungen** aktivieren (oder deaktivieren).

Schritt 4. Verwaltung der Updates von Drittherstellern konfigurieren

Dieser Schritt wird nicht angezeigt, wenn die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* bereits vorhanden ist.

Wenn Sie eine Liste mit Updates für die auf den verwalteten Geräten installierten Programme, sowie eine Liste mit gefundenen Schwachstellen mitsamt deren empfohlener Korrekturen, erhalten möchten, aktivieren Sie die Option **Nach Software-Updates von Drittherstellern und Patches zum Schließen von Schwachstellen suchen**. Bei aktivierter Option erstellt Kaspersky Next Expert View die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*.

Schritt 5. Erstellen einer grundlegenden Konfiguration für Netzwerkschutz

Klicken Sie in diesem Schritt des Assistenten auf **Erstellen**, um die für den grundlegenden Schutz Ihrer Client-Geräte benötigten Objekte zu erstellen.

Kaspersky Next Expert View Operator führt zwei Vorgänge aus:

- Die Erstellung grundlegender Richtlinien und Aufgaben mit Standardeinstellungen

  Die folgenden Richtlinien werden erstellt:

  - Die Richtlinie für den Kaspersky Security Center Administrationsagenten
  - Die Richtlinien für verwaltete Kaspersky-Anwendungen

  Die folgenden Aufgaben werden erstellt:

  - Die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*
  - Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*

    Diese Aufgabe wird nur erstellt, wenn Sie die Option **Nach Software-Updates von Drittherstellern und Patches zum Schließen von Schwachstellen suchen** im vorherigen Schritt des Assistenten aktiviert haben.
  - Die Aufgaben für verwaltete Kaspersky-Anwendungen

- Ein autonomes Installationspaket für den Administrationsagenten erstellen

  Dieses Paket werden Sie für die Installation des Administrationsagenten auf den Verteilungspunkten verwenden. Kaspersky Next Expert View erstellt das autonome Installationspaket auf Basis des Installationspakets des Administrationsagenten, welches Sie im vorhergehenden Schritt des Assistenten ausgewählt haben. Während der Erstellung des Pakets müssen Sie EULA-Bedingungen des Administrationsagenten durchlesen und akzeptieren. Wenn das autonome Installationspaket erstellt ist, werden Sie aufgefordert, es auf das Gerät herunterzuladen, welches Sie gerade verwenden.

  Das Erstellen eines autonomen Installationspakets für den Administrationsagenten kann etwas Zeit in Anspruch nehmen. Fahren Sie mit dem nächsten Schritt des Assistenten fort. Der Prozess wird im Hintergrund weiterhin ausgeführt. Bei Bedarf können Sie den Download-Status des Installationspakets in der Spalte **Paketstatus** (**Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete**) nachverfolgen.

Zu Authentifizierungszwecken wird jedes autonome Installationspaket unter Verwendung eines Zertifikats signiert. Das Zertifikat wird alle 3 Monate neu ausgestellt. Nach jeder erneuten Ausstellung eines Zertifikats aktualisiert Kaspersky Next Expert View die Signaturen aller erstellten autonomen Installationspakete automatisch. Für heruntergeladene autonome Installationspakete kann die automatische Aktualisierung der Signatur nicht erfolgen. Es kann daher passieren, dass das Zertifikat abläuft und bei der Installation eines Programms mittels eines autonomen Installationspakets ein Zertifikatfehler auftritt. Laden Sie in diesem Fall das autonome Installationspaket erneut herunter.

Sie können die Gültigkeitsdauer des Zertifikats in den Eigenschaften des autonomen Installationspakets anzeigen, das auf Ihr Gerät heruntergeladen wurde. Klicken Sie dazu mit der rechten Maustaste auf das autonome Installationspaket und öffnen Sie dessen Details. Wählen Sie auf der Registerkarte **Digitale Signaturen** das erforderliche Zertifikat in der Liste aus, klicken Sie auf die Schaltfläche **Details** und anschließend im neuen Fenster auf **Zertifikat anzeigen**.

Schritt 6. Schnellstartassistent abschließen

Lesen Sie sich auf der letzten Seite des Schnellstartassistenten die zusätzlichen Schritte durch, die Sie ausführen müssen, um Kaspersky-Sicherheitsanwendungen auf den Client-Geräten zu installieren. Folgen Sie dem angezeigten Szenario zur erstmaligen Bereitstellung von Kaspersky-Anwendungen.

Erstbereitstellung von Kaspersky-Anwendungen

Dieser Abschnitt beschreibt die Erstbereitstellung von Kaspersky-Anwendungen auf den Client-Geräten in Ihrem Unternehmen.

Szenario: Erstmalige Bereitstellung von Kaspersky-Programmen

Dieses Szenario beschreibt die Installation von Kaspersky-Anwendungen auf Client-Geräten mittels Kaspersky Next Expert View. Zunächst müssen Sie in Ihrem Netzwerk Verteilungspunkte bereitstellen. Anschließend müssen Sie mithilfe der Verteilungspunkte eine Netzwerkabfrage durchführen und vernetzte Geräte in Ihrem Netzwerk erkennen. Danach können Sie Kaspersky-Anwendungen auf den vernetzten Geräten bereitstellen.

Wenn das Szenario abgeschlossen ist, werden die Kaspersky-Anwendungen auf den ausgewählten Client-Geräten im Netzwerk Ihrer Organisation bereitgestellt. Sie können all diese Geräte mit installierten Kaspersky-Anwendungen verwalten.

Erforderliche Vorrausetzungen

Stellen Sie vor dem Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der Schnellstartassistent ist abgeschlossen.
- Installationspakete für den Administrationsagenten und die Sicherheitsanwendungen werden erstellt.
- Sie besitzen Informationen zu den Interneteinstellungen für die Client-Geräte in Ihrer Organisation, zu den Gateways und zu den Einstellungen des Proxyservers.
- Die Client-Geräte in Ihrem Unternehmen werden nicht verschlüsselt.

Schritte

Die Erstbereitstellung von Kaspersky-Anwendungen erfolgt schrittweise:

1. **Ein Gerät als Verteilungspunkt auswählen**

In Kaspersky Next Expert View ist ein Verteilungspunkt für Folgendes vorgesehen:

- Netzwerkabfrage und Gerätesuche
- Remote-Installation des Administrationsagenten auf Client-Geräten
- Verbindung von Client-Geräten mit dem Administrationsserver (wenn ein Verteilungspunkt als Verbindungs-Gateway fungiert)

Wählen Sie im Netzwerk Ihrer Organisation ein Gerät aus, das als Verteilungspunkt für eine Administrationsgruppe fungieren soll. Das ausgewählte Gerät muss die Voraussetzungen für Verteilungspunkte. Wählen Sie je nach Anzahl der Client-Geräte im Netzwerk Ihrer Organisation die passende Anzahl an Geräten aus, die als Verteilungspunkte fungieren sollen.

2. **Ein autonomes Installationspaket für den Administrationsagenten erstellen**

   Erstellen Sie ein autonomes Installationspaket für den Administrationsagenten, das auf dem Verteilungspunkt installiert wird.

   Wenn Ihre Client-Geräte keinen direkten Internetzugang für die Verbindung mit dem Administrationsserver haben, konfigurieren Sie in den Einstellungen des Installationspakets für den Administrationsagenten die Einstellungen des Verbindungs-Gateways und es Proxyservers.

3. **Installieren des Administrationsagenten auf dem ausgewählten Gerät, das als Verteilungspunkt fungieren soll**

   Übertragen Sie das autonomes Installationspaket für den Administrationsagenten auf beliebige Weise an das ausgewählte Gerät. Beispielsweise können Sie das autonomes Installationspaket auf einen Wechseldatenträger (z. B. ein USB-Laufwerk) kopieren oder es in einem freigegebenen Ordner ablegen.

   Stellen Sie im Fenster **Eigenschaften** der Datei des autonomen Installationspakets sicher, dass das autonome Installationspaket für den Administrationsagenten von Kaspersky signiert ist.

   Führen Sie die Installation des autonomen Installationspakets für den Administrationsagenten auf dem ausgewählten Gerät aus. Der Administrationsagent ist jetzt gemäß den Einstellungen des Installationspakets für den Administrationsagenten installiert und mit dem Administrationsserver verbunden. Das Gerät mit dem Administrationsagenten wird in die Administrationsgruppe verschoben, die bei der Erstellung des autonomen Installationspakets für den Administrationsagenten angegeben wurde.

   > Wenn Sie den Administrationsagenten unter Verwendung eines autonomen Installationspaketes auf einem Gerät mit Microsoft Windows XP Professional for Embedded Systems 32-Bit installieren, schlägt die Installation fehl. Um das Problem zu beheben, installieren Sie zuvor das Update KB2868626 für Windows XP von der Microsoft-Webseite: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

4. **Weisen Sie dem Gerät mit installiertem Administrationsagent die Rolle des Verteilungspunkts zu**

   Weisen Sie dem Gerät mit installiertem Administrationsagent die Rolle des Verteilungspunkts zu.

5. **Konfigurieren und Ausführen von Netzwerkabfragen mittels Verteilungspunkt**

   Konfigurieren Sie für den Verteilungspunkt mit installiertem Administrationsagenten die Netzwerkabfrage. Optional können Sie die Netzwerkabfrage in der Richtlinie des Administrationsagenten konfigurieren.

   Wenn die Netzwerkabfrage nach Zeitplan abgeschlossen wurde, sind die mit dem Netzwerk Ihrer Organisation verbundenen Client-Geräte entdeckt und in die Gruppe **Nicht zugeordnete Geräte** verschoben.

6. **Installationspakete für den Administrationsagenten und für verwaltete Kaspersky-Programme erstellen**

   Wenn Sie den Schnellstartassistenten nicht ausgeführt oder den Schritt zum Erstellen von Installationspaketen übersprungen haben, erstellen Sie Installationspakete für Kaspersky-Programme. Sie müssen sowohl für den Administrationsagenten als auch für die verwalteten Kaspersky-Anwendungen Installationspakete erstellen, die für das auf den Client-Geräten im Netzwerk Ihrer Organisation installierte Betriebssystem geeignet sind.

7. **Entfernen der Sicherheitsanwendung von Drittanbietern.**

   Wenn auf den Geräten im Netzwerk Ihrer Organisation Sicherheitsanwendung von Drittanbietern installiert sind, entfernen Sie diese, bevor Sie mit der Installation von Kaspersky-Anwendungen beginnen.

8. **Kaspersky-Anwendungen auf Client-Geräten installieren**

   Erstellen Sie Aufgaben, um den Administrationsagenten und verwaltete Kaspersky-Anwendungen auf den Client-Geräten im Netzwerk Ihrer Organisation zu installieren. Verwenden Sie beim Erstellen der Aufgaben den Aufgabentyp **Remote-Installation einer Anwendung**. Verwenden Sie für die Aufgabe zum Installieren des Administrationsagenten die Option **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**. Verwenden Sie für die Aufgabe zum Installieren verwalteter Kaspersky-Anwendungen die Option **Unter Nutzung des Administrationsagenten**. Nachdem die Aufgaben erstellt wurden, können Sie die Einstellungen konfigurieren. Stellen Sie sicher, dass der Zeitplan für jede erstellte Aufgabe Ihren Anforderungen entspricht. Zunächst muss die Aufgabe zum Installieren des Administrationsagenten ausgeführt werden. Nachdem der Administrationsagent auf Client-Gerät installiert wurde, muss die Aufgabe zum Installieren von verwalteten Kaspersky-Anwendungen ausgeführt werden.

   Optional können Sie eine Aufgabe zur Remote-Installation erstellen, um den Administrationsagenten und verwaltete Kaspersky-Anwendungen auf Client-Geräten im Netzwerk Ihrer Organisation zu installieren. Verwenden Sie in diesem Fall im Block **Installationspakete** die Option **Installationspaket auswählen** und die Option **Administrationsagent auswählen** und im Block **Download des Installationspakets erzwingen** die Option **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**.

   Darüber hinaus können Sie auch verschiedene Aufgaben zur Remote-Installation von verwalteten Kaspersky-Anwendungen für verschiedene Administrationsgruppen oder für unterschiedliche Geräteauswahlen erstellen.

   Wenn Sie über Client-Geräte verfügen, die sich außerhalb des Netzwerks mit Verteilungspunkt befinden, z. B. Laptops von Remote-Benutzern, müssen Sie das autonome Installationspaket für den Administrationsagenten erstellen und auf diesen Client-Geräten auf irgendeine Weise ausliefern. Installieren Sie das autonomes Installationspaket für den Administrationsagenten lokal auf diesen Client-Geräten. Anschließend können Sie auf den Geräten dieser Remote-Benutzer verwaltete Kaspersky-Anwendungen installieren, indem Sie denselben Anweisungen folgen wie für andere Geräte, die vom Verteilungspunkt erkannt wurden.

   Starten Sie die Aufgaben zur Remote-Installation.

   Alternativ dazu können Sie zur Installation von Kaspersky-Anwendungen den Assistent für die Bereitstellung des Schutzes starten.

9. **Installieren von Kaspersky Security für mobile Endgeräte**

   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.

10. **Überprüfung der Erstbereitstellung von Kaspersky-Programmen**

    Lassen Sie sich den **Bericht über Versionen der Kaspersky-Anwendungen** generieren und anzeigen. Stellen Sie sicher, dass die verwalteten Kaspersky-Anwendungen auf allen Client-Geräten in Ihrer Organisation installiert sind.

Für die vollständige Festplattenverschlüsselung wird von Kaspersky Next Expert View nur BitLocker unterstützt.

Erstellen von Installationspaketen für Kaspersky-Programme

Um Kaspersky-Anwendungen auf vernetzten Geräten in Ihrem Unternehmen bereitzustellen, müssen Sie Installationspakete für Kaspersky-Anwendungen in Kaspersky Next Expert View erstellen.

So erstellen Sie ein Installationspaket für eine Kaspersky-Anwendung:

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**.

   Sie können Benachrichtigungen über neue Pakete 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 eine Kaspersky-Anwendung erstellen**.

   Eine Liste der auf den Kaspersky-Webservern verfügbaren Programmpakete wird angezeigt. Standardmäßig werden in der Liste nur Anwendungen in Englisch sowie in der Sprache angezeigt, die der Schnittstelle entspricht. Um weitere Sprachen anzuzeigen, klicken Sie auf **„Filter“** und konfigurieren Sie die Filtereinstellungen.

4. Klicken Sie auf den Namen eines Programmpakets, z. B. **Kaspersky Endpoint Security für Windows (<Versionsnummer>)**.

   Ein Fenster mit Informationen über das Programmpaket wird geöffnet.

5. Lesen Sie die Informationen und klicken Sie auf **Herunterladen und Installationspaket erstellen**.

   Wenn ein Programmpaket nicht automatisch in ein Installationspaket konvertiert werden kann, wird die Schaltfläche **Programmpaket herunterladen** anstelle der Schaltfläche **Herunterladen und Installationspaket erstellen** angezeigt. Laden Sie in diesem Fall das Programmpaket herunter, und verwenden sie die heruntergeladene Datei zur Erstellung eines benutzerdefiniertes Installationspakets.

   Bei einigen Kaspersky-Anwendungen wird vor oder 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 die Lizenzverträge zu lesen.

   b. Lesen Sie im neuen Bereich die Lizenzverträge, die auf dem Bildschirm angezeigt werden.

      Um die von den Kaspersky-Anwendungen verarbeiteten Daten anzuzeigen, für die Sie ein Installationspaket erstellen möchten, klicken Sie auf **Liste der Daten anzeigen**.

   c. Wählen Sie die Lizenzverträge aus und klicken Sie anschließend auf **Akzeptieren**.

Der Download wird fortgesetzt, nachdem Sie die Lizenzverträge akzeptiert haben. Wenn Sie auf **Ablehnen** klicken, wird der Download beendet.

Sie können das Fenster des Assistenten schließen. In diesem Fall wird der Download im Hintergrund fortgesetzt. In der Spalte **Paketstatus** können Sie den Download-Status des Installationspakets verfolgen, sowie Filter anwenden und nach Status sortieren.

Wenn der Download-Prozess angehalten wird und sich der Status zu **EULA akzeptieren** ändert, klicken Sie auf den Namen des Installationspakets und führen Sie die Schritte 5.a und 5.b aus.

Standardmäßig werden die Installationspakete mit dem Status **In Bearbeitung** und **EULA akzeptieren** am Anfang der Liste platziert.

Wenn Sie planen, eine Migration von Kaspersky Security Center Web Console auf Kaspersky Next Expert View durchzuführen, und die Sicherheitsbestimmungen Ihres Unternehmens die Verwendung eines Proxys für den Zugriff auf das Unternehmensnetzwerk erfordern, kann sich dies auf den Migrationsprozess auswirken. Nachdem Sie ein Installationspaket des Administrationsagenten erstellt haben, müssen Sie die Proxy-Einstellungen angeben, um eine Verbindungsherstellung zwischen den Instanzen der Administrationsagenten auf den verwalteten Geräten und Ihrem Arbeitsbereich von Kaspersky Next Expert View sicherzustellen:

a. Klicken Sie auf den Namen des Installationspakets.

b. Wechseln Sie im sich öffnenden Eigenschaftenfenster für Installationspakete auf die Registerkarte **Einstellungen**.

c. Öffnen Sie den Abschnitt **Verbindung**.

d. Wählen Sie die Option **Proxyserver verwenden** und füllen Sie die Felder **Proxyserver-Adresse** und **Proxyserver-Port** aus.

6. Klicken Sie nach Abschluss des Downloads auf die Schaltfläche **Schließen** (), um das Fenster mit den Informationen über das Programmpaket zu schließen.

Das Installationspaket ist erstellt. Das Installationspaket wird in der Liste der Installationspakete aufgeführt.

Ein Installationspaket kann nur einmal in einer bestimmten Lokalisierungssprache hinzugefügt werden. Wenn Sie beispielsweise das Installationspaket für Kaspersky Endpoint Security für Windows (Deutsch) bereits hinzugefügt haben, können Sie weitere Installationspakete von Kaspersky Endpoint Security für Windows in anderen Sprachen hinzufügen. Das Paket für Deutsch können Sie jedoch nicht noch einmal hinzufügen.

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 Schritten des Assistenten.

   Wählen Sie im Feld **Aufgabentyp** des Fensters **Neue Aufgabe** des Assistenten für das Erstellen einer Aufgabe die Option **Installationspaket verteilen**. Sie können auch den Standardnamen der Aufgabe im Feld **Aufgabenname** ändern.

   Geben Sie im nächsten Schritt die sekundären Administrationsserver für den Aufgabenbereich an und folgen Sie den Anweisungen des Assistenten für das Erstellen einer Aufgabe. Wenn Sie den Assistenten für das Erstellen einer Aufgabe abschließen, erstellt dieser die Aufgabe zur Verteilung der gewählten Installationspakete auf die vorgesehenen sekundären Administrationsserver.

   > Wenn Sie für lokal ausgeführte sekundäre Administrationsserver eine Aufgabe zur Verteilung von Installationspaketen erstellen, umfasst die Verteilungsmenge – abgesehen von benutzerdefinierten Installationspaketen – ausschließlich Installationspakete, die von der lokal ausgeführten Kaspersky Security Center Web Console unterstützt werden, unabhängig davon, welche Verteilungsoption gewählt wurde (**Alle Installationspakete** oder **Ausgewählte Installationspakete**).

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.

Erstellen eines autonomes Installationspakets für den Administrationsagenten

Autonome Installationspakete können von Ihnen und von Gerätebenutzern in Ihrem Unternehmen verwendet werden, um den Administrationsagenten lokal auf Geräten zu installieren. Autonome Installationspakete können für Geräte mit Windows, Linux oder macOS erstellt werden.

In Kaspersky Next Expert View können Sie autonome Installationspakete nur für den Administrationsagenten erstellen.

Bei einem autonomen Installationspaket handelt es sich um eine ausführbare Datei, die per E-Mail verschickt oder auf eine andere Weise auf ein Client-Gerät übermittelt werden kann. Die empfangene Datei kann lokal auf dem Client-Gerät gestartet werden, um den Administrationsagenten ohne Beteiligung von Kaspersky Next Expert View zu installieren.

Für die Administrationsagenten für Linux und macOS ist das autonome Installationspaket eine Skriptdatei mit der Erweiterung .sh. Wenn Sie diese Datei ausführen, entpackt das Skript das angehängte Archiv, welches das Installationspaket und seine Einstellungen enthält, und startet anschließend die Installation.

Wenn der Administrationsserver Zugriff auf das Internet hat, wird die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** dazu verwendet, die Abhängigkeiten herunterzuladen, die zur Erstellung des autonomen Installationspakets des Administrationsagenten erforderlich sind. Wenn der Administrationsserver keinen Zugriff auf das Internet hat, führen Sie die folgenden Schritte aus:

1. Führen Sie den folgenden Befehl aus, um das Flag "RIUtilsArchiveDirUsed" zu erstellen:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Führen Sie den folgenden Befehl aus, um den Dienst des Administrationsservers neu zu starten:

   ```
   systemctl restart kladminserver_srv.service
   ```

Laden Sie die folgenden Archive von der Kaspersky-Website herunter und platzieren Sie die Archive im Ordner /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives:

- ri_utils_win32.zip
- ri_utils_arm64.zip

Benennen Sie die Archive nicht um.

Der Administrationsserver verfügt nun über die erforderlichen Abhängigkeiten.

Wenn Sie den Administrationsagenten unter Verwendung eines autonomen Installationspaketes auf einem Gerät mit Microsoft Windows XP Professional for Embedded Systems 32-Bit installieren, schlägt die Installation fehl. Um das Problem zu beheben, installieren Sie zuvor das Update KB2868626 für Windows XP von der Microsoft-Webseite: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

Zu Authentifizierungszwecken wird jedes autonome Installationspaket unter Verwendung eines Zertifikats signiert. Das Zertifikat wird alle 3 Monate neu ausgestellt. Nach jeder erneuten Ausstellung eines Zertifikats aktualisiert Kaspersky Next Expert View die Signaturen aller erstellten autonomen Installationspakete automatisch. Für heruntergeladene autonome Installationspakete kann die automatische Aktualisierung der Signatur nicht erfolgen. Es kann daher passieren, dass das Zertifikat abläuft und bei der Installation eines Programms mittels eines autonomen Installationspakets ein Zertifikatfehler auftritt. Laden Sie in diesem Fall das autonome Installationspaket erneut herunter.

Sie können die Gültigkeitsdauer des Zertifikats in den Eigenschaften des autonomen Installationspakets anzeigen, das auf Ihr Gerät heruntergeladen wurde. Klicken Sie dazu mit der rechten Maustaste auf das autonome Installationspaket und öffnen Sie dessen Details. Wählen Sie auf der Registerkarte **Digitale Signaturen** das erforderliche Zertifikat in der Liste aus, klicken Sie auf die Schaltfläche **Details** und anschließend im neuen Fenster auf **Zertifikat anzeigen**.

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 Installationspakete wird angezeigt. Wenn das Installationspaket für den Administrationsagenten nicht in der Liste enthalten ist, erstellen Sie es manuell.

2. Klicken Sie in der Liste der Installationspakete auf den Namen des Installationspakets für den Administrationsagenten.

   Das Eigenschaftenfenster des Installationspakets des Administrationsagenten wird angezeigt.

3. Konfigurieren Sie gegebenenfalls die Einstellungen des Installationspaketes des Administrationsagenten und schließen Sie dann das Eigenschaftenfenster.

4. Wählen Sie in der Liste der Installationspakete ein Installationspaket aus und klicken Sie oberhalb der Liste auf **Bereitstellen**.

5. 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.

6. Stellen Sie sicher, dass die Option **Administrationsagent gemeinsam mit dieser Anwendung installieren** aktiviert ist, wenn Sie den Administrationsagenten zusammen mit dem ausgewählten Programm installieren möchten.

   > Die Option wird abhängig von der Anwendung angezeigt, für die Sie ein autonomes Installationspaket erstellen.

   Diese Option ist standardmäßig aktiviert. Es wird empfohlen, 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.

7. Standardmäßig ist im Schritt **In die Liste mit verwalteten Geräten verschieben** die Option **Geräte nicht verschieben** ausgewählt. Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten nicht in Administrationsgruppen verschieben möchten, ändern Sie die Auswahl der Option nicht.

   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.

8. Wählen Sie die Option **Liste der autonomen Pakete öffnen** aus, wenn nach Abschluss des Assistenten die Liste der autonomen Installationspakete angezeigt werden soll.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets beendet.

Das autonome Installationspaket für den Administrationsagenten wird erstellt. Das erstellte autonome Installationspaket wird in der Liste mit den autonomen Installationspaketen angezeigt, die Sie auch aufrufen können.

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:

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 Installationspakete wird angezeigt.

2. Klicken Sie oberhalb der Liste auf die Schaltfläche **Liste der autonomen Pakete anzeigen**.

Eine Liste mit autonomen Installationspaketen wird angezeigt.

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.
- **Installationspaket-Name des Administrationsagenten**.
- **Version des Administrationsagenten**.
- **Größe**. Dateigröße in Megabyte (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.
- **Datei-Hash**. Mit dieser Eigenschaft wird bestätigt, dass das autonome Installationspaket nicht von Dritten verändert wurde und dass 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:

- Löschen Sie ein autonomes Installationspaket, indem Sie auf die Schaltfläche **Entfernen** klicken.
- Laden Sie ein autonomes Installationspaket auf Ihr Gerät herunter, indem Sie auf die Schaltfläche **Herunterladen** klicken.

  Zu Authentifizierungszwecken wird jedes autonome Installationspaket unter Verwendung eines Zertifikats signiert. Das Zertifikat wird alle 3 Monate neu ausgestellt. Nach jeder erneuten Ausstellung eines Zertifikats aktualisiert Kaspersky Next Expert View die Signaturen aller erstellten autonomen Installationspakete automatisch. Für heruntergeladene autonome Installationspakete kann die automatische Aktualisierung der Signatur nicht erfolgen. Es kann daher passieren, dass das Zertifikat abläuft und bei der Installation eines Programms mittels eines autonomen Installationspakets ein Zertifikatfehler auftritt. Laden Sie in diesem Fall das autonome Installationspaket erneut herunter.

  Sie können die Gültigkeitsdauer des Zertifikats auch in den Eigenschaften des heruntergeladenen autonomen Installationspakets anzeigen. Dazu müssen Sie auf der Registerkarte **Digitale Signaturen** das erforderliche Zertifikat in der Liste auswählen, auf die Schaltfläche **Details** klicken und im neuen Fenster auf **Zertifikat anzeigen** klicken.

Erstellen benutzerdefinierter Installationspakete

Sie können benutzerdefinierte Installationspakete für Folgendes verwenden:

- Zum Installieren eines beliebigen Programms (z. B. eines Texteditors) auf einem Client-Gerät, auf dem Kaspersky Next Expert View installiert ist, z. B. über eine Aufgabe.
- Zum Erstellen eines autonomen Installationspakets.

Ein benutzerdefiniertes Installationspaket ist ein Ordner mit einer Reihe von Dateien, einschließlich einer ausführbaren Datei. Eine Quelle zum Erstellen eines benutzerdefinierten Installationspakets ist eine Archivdatei. Die Archivdatei enthält Dateien, die im benutzerdefinierten Installationspaket enthalten sein müssen. Wenn Sie ein benutzerdefiniertes Installationspaket erstellen, können Sie Befehlszeilenparameter angeben, z. B. um das Programm im Silent-Modus zu installieren.

Im Testmodus von Kaspersky Next Expert View können Sie keine benutzerdefinierten Installationspakete erstellen.

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 das Erstellen eines Installationspakets 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 Installationspakets an und klicken Sie auf die Schaltfläche **Durchsuchen**.

   Im Standardfenster **Öffnen** können Sie eine Archivdatei zum Erstellen des Installationspakets auswählen.

5. Wählen Sie die gewünschte Archivdatei aus.

   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.

   Die Dateien werden auf dem Administrationsserver von Kaspersky Next Expert View heruntergeladen.

   Wenn der Administrationsserver feststellt, dass das Archiv eine Kaspersky-Anwendung enthält, wird eine Fehlermeldung angezeigt. Sie können Installationspakete für Kaspersky-Anwendungen von den Kaspersky-Webservern herunterladen. Dieser Vorgang steht unter **Vorgänge → Kaspersky-Anwendungen → Aktuelle Anwendungsversionen** zur Verfügung.

6. Wenn die ausgewählte Archivdatei mehrere ausführbare Dateien enthält, wählen Sie eine ausführbare Datei aus, die gestartet werden soll, um das Programm mithilfe des erstellten Installationspakets zu installieren.

7. Sie können Befehlszeilenparameter für eine ausführbare Datei angeben.

   Sie können bestimmte Befehlszeilenparameter angeben, um das Programm im Silent-Modus aus dem Installationspaket zu installieren. Details über die Befehlszeilenparameter finden Sie in der Dokumentation des Programmherstellers.

   Das Erstellen des Installationspakets beginnt.

   Der Assistent meldet, wenn der Vorgang abgeschlossen ist.

   Wenn das Installationspaket nicht erstellt wurde, wird eine Fehlermeldung angezeigt.

In Kaspersky Next Expert View ist die Gesamtgröße aller benutzerdefinierten Installationspakete auf dem Administrationsserver auf 500 MB begrenzt. Wird dieses Limit beim Erstellen eines neuen benutzerdefinierten Installationspakets überschritten, löschen Sie ältere, zuvor erstellte benutzerdefinierte Installationspakete. Die Größe eines Installationspakets wird in seinen Eigenschaften angezeigt.

8. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Assistenten zu schließen.

Das erstellte benutzerdefinierte Installationspaket wird auf den Administrationsserver heruntergeladen. Nach dem Herunterladen erscheint das Installationspaket in der Liste der Installationspakete.

In der Liste der Installationspakete können Sie die folgenden Eigenschaften eines benutzerdefinierten Installationspakets einsehen:

- **Name**. Der Name des benutzerdefinierten Installationspakets.
- **Paketstatus**. Downloadstatus des Installationspakets.
- **Quelle**. Der Hersteller der Anwendung.
- **Anwendung**. Die im benutzerdefinierten Installationspaket enthaltene Anwendung.
- **Version**. Version der Anwendung.
- **Sprache**. Sprache der Anwendung, die im benutzerdefinierten Installationspaket enthalten ist.
- **Größe (MB)**. Größe des benutzerdefinierten Installationspakets.
- **Betriebssystem**. Betriebssystem, für welches das benutzerdefinierte Installationspaket erstellt wurde.
- **Erstellt**. Erstellungsdatum des Installationspakets.
- **Geändert**. Änderungsdatum des Installationspaketes.
- **Typ**. Kaspersky-Anwendung oder Drittanbieteranwendung.

In der Liste der Installationspakete können Sie durch Anklicken des Links mit dem Namen eines benutzerdefinierten Installationspakets die Befehlszeilenparameter und den Namen des benutzerdefinierten Installationspakets ändern.

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.

Ein Verteilungspunkt benötigt außerdem Internetzugang und muss immer verbunden sein.

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.

Einstellungen des Installationspakets des Administrationsagenten

Um die Einstellungen des Installationspakets des Administrationsagenten anzupassen, gehen Sie wie folgt vor:

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 den Link mit dem Namen des Installationspakets für den Administrationsagenten.

   Das Eigenschaftenfenster des Installationspakets für den Administrationsagenten wird geöffnet. Die Informationen im Fenster sind in Registerkarten und in Abschnitten gruppiert.

Allgemein

Der Abschnitt **Allgemein** enthält allgemeine Informationen zum Installationspaket:

- Sprache des Installationspakets
- 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**

- **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 dieses Kontrollkästchen aktiviert ist, werden alle heruntergeladenen Updates und Patches für den Administrationsagenten automatisch installiert.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden die heruntergeladenen Updates und Patches nur installiert, sobald Sie deren Status auf *Genehmigt* setzen. Updates und Patches mit dem Status *Nicht festgestellt* werden nicht installiert.

  Dieses Kontrollkästchen ist standardmäßig ausgewählt.

Verbindung

In diesem Abschnitt können Sie die Einstellungen für die Verbindung des Administrationsagenten mit dem Administrationsserver anpassen:

- **UDP-Port verwenden**

  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.

- **Keinen Proxyserver verwenden**

- **Proxyserver verwenden**

  Wenn diese Option aktiviert ist, wird ein Internet-Proxyserver verwendet, um den Administrationsagenten mit dem Administrationsserver und einem Verbindungs-Gateway zu verbinden.

  Proxyserver-Adresse

  Proxyserver-Port

- **Authentifizierung am Proxyserver**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern 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.

  Benutzername

  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.

Aus Kompatibilitätsgründen wird es nicht empfohlen, die Einstellungen der Proxy-Verbindung in den Einstellungen des Installationspakets für den Administrationsagenten festzulegen.

Erweitert

In diesem Abschnitt können Sie sowohl konfigurieren, wie das Verbindungs-Gateway und die virtuelle Maschine verwendet werden, als auch angeben, ob ein Benutzer als Gerätebesitzer registriert werden soll:

- **Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen**

  Es wird nur eine direkte Verbindung zu Verbindungs-Gateways unterstützt. Die im Installationspaket angegebene Option zur Verwendung eines Internet-Proxyservers wird nicht angewendet.

- **Adresse des Verbindungs-Gateways**

- **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 des Kontrollkästchens **Ports des Administrationsagenten in der Windows-Firewall öffnen**	✓ * mit Ausnahme des Kontrollkästchens **Ports des Administrationsagenten in der Windows-Firewall öffnen**
Erweitert	✓	✓	✓
Zusätzliche Komponenten	✓	✓	✓
Tags	✓	✓ * mit Ausnahme der Regeln zur automatischen Zuweisung von Tags	✓ * mit Ausnahme der Regeln zur automatischen Zuweisung von Tags
Revisionsverlauf	✓	✓	✓

Virtuelle Infrastruktur

Kaspersky Next Expert View unterstützt die Arbeit mit virtuellen Maschinen. Um Ihre virtuelle Infrastruktur zu schützen, müssen Sie den Administrationsagenten auf jeder virtuellen Maschine installieren.

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 Next Expert View 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 Next Expert View 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. Die virtuelle Maschine mit dem installiertem Administrationsagenten wird auch der Administrationsserver-Datenbank hinzugefügt. Nach dem Deaktivieren dieser virtuellen Maschine muss der sie betreffende Eintrag auch aus der Administrationsserver-Datenbank 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

Kaspersky Next Expert View unterstützt das Kopieren von virtuellen Maschinen mit installiertem Administrationsagenten und das Erstellen virtueller Maschinen aus einer Vorlage mit installiertem Administrationsagenten.

Der Administrationsagent kann das Kopieren von virtuellen Maschinen in den folgenden Fällen automatisch erkennen:

- 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.

Administrationsagent für Windows, Linux und macOS: Vergleich

Der Administrationsagent für macOS und Linux weist im Vergleich zum Administrationsagenten für Windows einige Einschränkungen auf. 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.

Vergleich der Funktionen des Administrationsagenten

Funktion des Administrationsagenten	Windows	Linux	macOS
Installation			
Automatische Installation von Updates und Patches für den Administrationsagenten	✓	✓	–
Automatische Verteilung von Schlüsseln	✓	✓	✓

Funktion des Administrationsagenten	Windows	Linux	macOS
Installation durch manuelles Starten der Installer der Programme auf den Geräten	✓	✓	✓
Erzwungene Synchronisierung	✓	✓	✓ Außer Push-Server
Verteilungspunkt			
Netzwerkabfrage	✓ • IP-Bereiche abfragen • Windows-Netzwerkabfrage • Abfrage des Domänencontrollers (Microsoft Active Directory)	✓ • IP-Bereiche abfragen • Abfrage des Domänencontrollers (Microsoft Active Directory, Samba 4 als Active Directory, FreeIPA und ALD Pro)	–
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	✓	✓	– 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.
Push-Installation von Programmen	✓	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.
Umgang mit Anwendungen von Drittanbietern			
Remote-Installation von Programmen auf Geräten	✓	–	–
Software-Updates	✓	–	–
Anpassen von Updates des Betriebssystems in einer Richtlinie des Administrationsagenten	✓	–	–
Informationen über Schwachstellen in Programmen anzeigen	✓	–	–
Schwachstellensuche in Programmen	✓	–	–
Inventarisierung von auf Geräten installierten Programmen	✓	✓	–
Virtuelle Maschinen			
Installation des Administrationsagenten auf einer virtuellen Maschine	✓	✓	✓
Einstellungen für Optimierung der Virtual Desktop Infrastructure (VDI)	✓	✓	✓

Funktion des Administrationsagenten	Windows	Linux	macOS
Unterstützung von dynamischen virtuellen Maschinen	✓	✓	✓
Anderes			
Audit von Aktionen auf einem Remote-Client-Gerät mithilfe der Windows Desktopfreigabe	✓	–	–
Verwaltung von Geräteneustarts	✓	–	–
Verbindungsmanager	✓	✓	✓
Verbindungsprofile für mobile Benutzer	✓	✓	✓
Remotedesktopverbindung mit dem Client-Gerät herstellen	✓	✓	✓

Die folgenden Abschnitte werden in den Eigenschaften des Verteilungspunkts zwar angezeigt, aber ihre entsprechenden Funktionen vom Administrationsagenten unter macOS nicht unterstützt:

- Update-Quelle
- KSN-Proxyserver
- Windows-Domänen
- Active Directory
- IP-Bereiche
- Erweitert
- Statistik

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 **Asset-Verwaltung** → **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 **Anwendungseinstellungen** → **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 Next Expert View 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 Next Expert View verwendet das Benutzerkonto oder das angegebene Kennwort nicht, um eine SSH-Verbindung herzustellen.

- **Geben Sie den Pfad eines temporären Ordners an, der sich auf dem Zielgerät befindet und die "Execute"-Berechtigung besitzt (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 Next Expert View 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.

Ersetzen von Sicherheitsanwendungen von Drittanbietern

Zur Installation der Sicherheitsanwendungen von Kaspersky mithilfe von Kaspersky Next Expert View ist es möglicherweise erforderlich, Drittanbieter-Programme zu löschen, die mit dem zu installierenden Programm nicht kompatibel ist. Kaspersky Next Expert View bietet mehrere Methoden zur Deinstallation von Drittanbieter-Programmen.

Inkompatible Programme während der Konfiguration der Remote-Installation eines Programms entfernen

Sie können die Option **Inkompatible Anwendungen automatisch entfernen** aktivieren, wenn Sie die Remote-Installation einer Sicherheitsanwendung konfigurieren. Diese Option finden Sie im Assistenten für die Bereitstellung des Schutzes. Wenn diese Option aktiviert ist, entfernt Kaspersky Next Expert View inkompatible Programme vor der Installation einer Sicherheitsanwendung auf dem verwalteten Gerät.

Löschen der inkompatiblen Programme mithilfe einer separaten Aufgabe

Zum Löschen der inkompatiblen Programme mithilfe einer Aufgabe wird die Aufgabe **Remote-Deinstallation des 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 Beenden einer anderen Aufgabe** ausgewählt werden, wobei die andere Aufgabe die Aufgabe **Remote-Deinstallation des Programms** ist.

Die Verwendung dieser Löschmethode ist zweckmäßig, wenn der Installer der Sicherheitsanwendung eines der inkompatiblen Programme nicht erfolgreich löschen kann.

Funktion zur manuellen Installation von Apps

Sie können den Administrationsagenten auf Geräten lokal installieren, ohne Kaspersky Next Expert View dafür zu verwenden. Erstellen Sie dazu, ein eigenständiges Installationspaket für den Administrationsagenten, wie im folgenden Artikel beschrieben: Autonome Installationspakete erstellen. Übertragen Sie das Paket auf Ihr Client-Gerät und installieren Sie es. Sobald die Installation des Administrationsagenten abgeschlossen ist, können Sie das Gerät als Verteilungspunkt verwenden.

Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Cloud Console

Um die erstmalige Bereitstellung des Administrationsagenten oder von anderen Anwendungen durchzuführen, können Sie die Installation der ausgewählten Installationspakete mithilfe der Aufgabe zur Remote-Installation der Kaspersky Next Expert View erzwingen. Voraussetzung dafür ist jedoch, dass jedes Gerät über mindestens ein Benutzerkonto mit lokalen Administratorrechten verfügt.

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 die Verteilungspunkte verteilen.

Sie müssen in den Einstellungen der Aufgabe zur Remote-Installation ein Benutzerkonto angeben, das Zugriff auf die Freigabe "admin$" hat.

Angeben können Sie die Geräte entweder explizit (mittels Liste), indem Sie die Administrationsgruppe von Kaspersky Next Expert View 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 Next Expert View ausgeführt. Dabei müssen die folgenden Bedingungen erfüllt werden:

- Die Zielgeräte sind vom Verteilungspunkt aus verfügbar.
- 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 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 Next Expert View 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.

Geräte, die als Verteilungspunkte fungieren, müssen den Voraussetzungen für Verteilungspunkte entsprechen. Sie müssen sicherstellen, dass die Verteilungspunkte in jedem isolierten Netzwerk vorhanden sind, in dem sich die Geräte befinden.

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.

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 einer Anwendung**.

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 aus, wie Sie das ausgewählte Installationspaket installieren möchten:

- **Remote-Installation mittels Kaspersky Security Center**
- **Remote-Installation mittels API von Microsoft Azure**

Wählen Sie anschließend das Installationspaket des Programms, das Sie installieren möchten.

Wenn das Installationspaket des gewünschten Programms nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie dann das Programm aus der Liste aus.

Schritt 3. 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 4. 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 5. Einstellungen für die Aufgabe zur Remote-Installation festlegen

Geben Sie im Fenster **Einstellungen für die Aufgabe "Remote-Installation"** die Einstellungen für die Remote-Installation eines Programms an.

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.

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 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.

Deinstallationskennwort der aktuellen Kaspersky-Anwendung

> Das Feld **Deinstallationskennwort der aktuellen Kaspersky-Anwendung** ist nur verfügbar, wenn Sie die Option **Unter Nutzung des Administrationsagenten** in der Einstellungsgruppe **Download des Installationspakets erzwingen** ausgewählt haben.

Geben Sie im Feld **Deinstallationskennwort der aktuellen Kaspersky-Anwendung** das Kennwort ein, wenn Sie von einer Kaspersky-Anwendung zu einem anderen migrieren und Ihre aktuelle Anwendung durch ein Kennwort geschützt ist. Beachten Sie, dass Ihre aktuelle Kaspersky-Anwendung während der Migration deinstalliert wird.

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.

Schritt 6. 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 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.

  - **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 7. 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 Next Expert View 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 8. 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 9. 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 Konto oder Domänenkonto**. 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 Konto oder Domänenkonto** 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 Next Expert View 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 Next Expert View 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 10. Beginnen der Installation

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.

Netzwerkeinstellungen zur Interaktion mit externen Diensten

Kaspersky Next Expert View 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 Next Expert View, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung 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
Port: 80 Protokoll: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Public Key-Infrastruktur (PKI)
Port: 443 Protokoll: HTTPS	https://ipm-klca.kaspersky.com	Marketing-Mitteilungen.

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 443 Protokoll: HTTPS	https://tip.kaspersky.com	Mittels Kaspersky Threat Intelligence Portal auf Bedrohungen reagieren (bei Verwendung der Funktionalitäten von Kaspersky Next XDR Optimum).
Port: 443 Protokoll: HTTPS	Eine vollständige Liste der Adressen finden Sie im Artikel Adresse und Domainstruktur.	Mittels Kaspersky Automated Security Awareness Platform reagieren (bei Verwendung der Funktionalitäten von Kaspersky Next XDR Optimum).

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 Next Expert View 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.

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.

   Wenn Sie Kaspersky Industrial CyberSecurity für Linux-Knoten auf einem Gerät mit einem Linux-Betriebssystem mit glibc 2.5 installieren müssen, müssen Sie eines der folgenden Installationspakete von der Kaspersky-Website:

   - klnagent64_16.1.0-5840_amd64_glibc2.5.deb
   - klnagent64-16.1.0-5840.x86_64_glibc2.5.rpm
   - klnagent_16.1.0-5840_i386_glibc2.5.deb
   - klnagent-16.1.0-5840.i386_glibc2.5.rpm

   Diese Installationspakete sind für die folgenden Betriebssysteme mit glibc 2.5 verfügbar:

   - CentOS 5.2 32-Bit/64-Bit
   - CentOS 5.4 32-Bit/64-Bit
   - CentOS 6.4 32-Bit/64-Bit
   - CentOS 6.6 32-Bit/64-Bit
   - Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.4) 64-Bit

   Um das Installationspaket zu erhalten, müssen Sie über eine Lizenz für Kaspersky Industrial CyberSecurity for Linux Nodes verfügen.

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.

      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.

   b. Deaktivieren Sie das Kennwort der sudo-Abfrage für das Benutzerkonto, das für die Verbindung mit dem Gerät verwendet wird.

   c. 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`

   d. Speichern und schließen Sie die Datei sudoers.

   e. 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`.

Programme mittels Aufgabe zur Remote-Installation installieren

In Kaspersky Next Expert View können Sie mit der Aufgabe zur Remote-Installation Programme auf Geräten remote-installieren. Diese Aufgaben werden mithilfe eines speziellen Assistenten 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**. In diesem Fall können Sie die DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die 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 standardmäßig erstellte 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 Next Expert View.

Eines Programm remote installieren

Dieser Artikel enthält Informationen darüber, wie ein Programm auf den Geräten einer Administrationsgruppe, auf Geräten mit bestimmten Adressen oder auf einer Auswahl an Geräten remote installiert wird.

Um ein Programm auf ausgewählten Geräten zu installieren:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **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 einer Anwendung** 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 aus, wie Sie das ausgewählte Programm installieren möchten:

     - **Remote-Installation mittels Kaspersky Security Center**

     - **Remote-Installation mittels API von Microsoft Azure**

       Weitere Informationen zur Installation von Programmen auf virtuellen Maschinen von Microsoft Azure finden Sie unter Remote-Installation von Programmen auf virtuellen Maschinen von Azure.

   - Wählen Sie im Feld **Installationspaket auswählen** das Installationspaket eines Programms, das Sie installieren möchten.

   - 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.

- 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 Next Expert View den Installer auf dem Gerät nicht mehr. Um die Aufgabe *Remote-Installation eines Programms* erneut zu starten, erhöhen Sie den Wert für den Parameter **Maximale Anzahl der Installationsversuche** und starten Sie die Aufgabe anschließend erneut. Alternativ dazu können Sie eine neue Aufgabe zur *Remote-Installation eines Programms* 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 **Deinstallationskennwort der aktuellen Kaspersky-Anwendung** ein Beachten Sie, dass Ihre aktuelle Kaspersky-Anwendung während der Migration deinstalliert wird.

  Das Feld **Deinstallationskennwort 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 kann bei der Installation weiterer Anwendungen 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.

- Geben Sie die erweiterte Optionen 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 überprüfen**

    Bevor die Dateien auf die Client-Geräte übertragen werden, prüft Kaspersky Next Expert View, ob die Einstellungen des Installationstools auf dem Betriebssystem des Client-Geräts anwendbar sind. Wenn die Einstellungen nicht anwendbar sind, überträgt Kaspersky Next Expert View die Dateien nicht und wird nicht versuchen, die Anwendung zu installieren. So können Sie beispielsweise ein Programm 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 ein Verteilungspunkt das Betriebssystem des Geräts automatisch, unabhängig davon, welchen Wert die Einstellung **Typ des Betriebssystems vor dem Download überprüfen** hat.

  - **Benutzer auffordern, laufende Anwendungen 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.

  Die Option **Geräte nicht verschieben** ist standardmäßig festgelegt. Aus Sicherheitsgründen sollten Sie die Geräte manuell verschieben.

7. Geben Sie in diesem Schritt des Assistenten an, ob die Geräte während der Installation von Programm neu gestartet werden sollen:

   - **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**

     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 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.

     - **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 Konto oder Domänenkonto**. 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 Konto oder Domänenkonto** 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 Next Expert View 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 Next Expert View 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.

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 einer Anwendung 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.

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 **Asset-Verwaltung** → **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 **Anwendung** die Anwendung aus, für welche Sie die Aufgabe erstellen möchten.
4. Wählen Sie in der Liste **Aufgabentyp** die Aufgabe **Anwendung starten/beenden** 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, denen die Aufgabe zugewiesen werden soll.

7. Gehen Sie im Fenster **Anwendungen** wie folgt vor:

   - Aktivieren Sie die Kontrollkästchen neben den Namen der Anwendungen, für die Sie die Aufgabe erstellen möchten.

   - Wählen Sie die Option **Anwendung starten** oder **Anwendung 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.

Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

Verwaltung mobiler Geräte

Die Verwaltung von mobilen Geräten mittels Kaspersky Next Expert View erfolgt mithilfe der Funktion "Verwaltung mobiler Geräte". 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 Security für mobile Endgeräte" gewährleistet, die auf den Geräten installiert ist. Diese App gewährleistet den Schutz mobiler Geräte vor Web-Bedrohungen, Viren und anderen Programmen, die Bedrohungen darstellen.

iOS-Geräte

Kaspersky Device Management für iOS gewährleistet den Schutz und die Kontrolle mobiler Geräte, die mit Kaspersky Next Expert View verbunden sind.

Die App von Kaspersky Security für iOS bietet die folgenden wichtigsten Funktionen:

- **Web-Schutz**. Diese Komponente blockiert schädliche Websites, die angelegt wurden, um schädlichen Code zu verbreiten. Der Web-Schutz blockiert zudem gefälschte Websites (Phishing-Sites), die vertrauliche Daten von Benutzern (etwa Kennwörter für Online-Banking oder E-Money-Systeme) abgreifen und auf die Finanzdaten von Benutzern zugreifen.

- **Jailbreak-Erkennung**. Wenn Kaspersky Security für iOS einen Jailbreak erkennt, zeigt es eine kritische Meldung an und informiert Sie über das Problem.

Informationen über die Bereitstellung des Schutzes und die Verwaltung mobiler Geräte finden Sie in der Hilfe zu Basic MDM in Kaspersky Next Expert View (Cloud).

Möglichkeiten von Detection and Response

Kaspersky Next Expert View kann die Funktionen anderer Kaspersky-Lösungen in der Benutzeroberfläche der Konsole integrieren. Beispielsweise können Sie Funktionalitäten für Detection and Response zu den Funktionen von Kaspersky Next Expert View hinzufügen.

Die Detection and Response-Lösungen dienen dem Schutz der IT-Infrastruktur eines Unternehmens vor komplexen Cyberbedrohungen. Die Funktionalität der Lösung kombiniert die automatische Erkennung von Bedrohungen (Detection) mit der Fähigkeit, auf diese Bedrohungen zu reagieren (Response), um komplexen Angriffen zu widerstehen – einschließlich neuartiger Exploits, Ransomware, dateiloser Angriffe und Methoden, die legitime Systemtools ausnutzen.

Integrierbare Lösungen

Kaspersky Endpoint Detection and Response Optimum

Nachdem ein Programm aus der Kaspersky Endpoint Protection Platform (auch als EPP bezeichnet) eine Bedrohung erkennt, fügt Kaspersky Next Expert View der Alarm-Liste einen neuen Alarm hinzu. Ein Alarm enthält detaillierte Informationen über die erkannte Bedrohung und ermöglicht es Ihnen, die Bedrohung zu analysieren und zu untersuchen. Außerdem können Sie den Vorfall visualisieren, indem Sie ein Diagramm zur Entwicklungskette der Bedrohung erstellen. Dieses Diagramm gibt die Phasen der Verbreitung des erkannten Angriffs in Relation zum Zeitverlauf wieder.

Als Reaktion können Sie eine der vordefinierten Reaktionsmaßnahmen auswählen, beispielsweise eine Datei in die Quarantäne verschieben, ein kompromittiertes Gerät vom Netzwerk isolieren oder eine Regel zur Verhinderung der Ausführung für ein nicht vertrauenswürdiges Objekt erstellen.

Weitere Informationen zur Aktivierung der Lösung finden Sie in der Dokumentation zu Kaspersky Endpoint Detection and Response Optimum.

Kaspersky Managed Detection and Response

Nachdem eine EPP-Anwendung von Kaspersky eine Bedrohung erkennt, fügt Kaspersky Next Expert View einen neuen Vorfall zur Vorfall-Liste hinzu. Ein Vorfall enthält detaillierte Informationen über die erkannte Bedrohung. Die Analysten des MDR Security Operation Center (SOC) von Kaspersky oder von einem Drittunternehmen untersuchen die Vorfälle und stellen Reaktionen zur Lösung der Vorfälle zur Verfügung. Sie können diese angebotenen Maßnahmen entweder manuell akzeptieren oder ablehnen, oder eine Option aktivieren, alle Reaktionen automatisch zu akzeptieren.

Weitere Informationen zur Aktivierung der Lösung finden Sie in der Dokumentation zu Kaspersky Managed Detection and Response.

Kaspersky Endpoint Detection and Response Expert

Dies ist eine Lösung für Unternehmen mit einem Team von SOC-Analysten. Erkannte Bedrohungen werden als Warnungen oder Vorfälle registriert, die SOC-Analysten zur Untersuchung zugewiesen werden können. Kaspersky Endpoint Detection and Response Expert bietet Ihnen detaillierte Informationen zu jedem Alarm oder Vorfall sowie Tools für die Verwaltung von Alarmen und Vorfällen, zum Threat Hunting und zur Entwicklung benutzerdefinierter Regeln. Die SOC-Analysten oder Security Officer können Response-Maßnahmen manuell auswählen oder die vordefinierten automatisierten Response-Maßnahmen einleiten.

Weitere Informationen zur Aktivierung der Lösung finden Sie in der Dokumentation zu Kaspersky Endpoint Detection and Response Expert.

Änderungen in der Benutzeroberfläche nach der Integration von Detection and Response

In der folgenden Tabelle sind die Änderungen aufgeführt, welche die Lösungen nach ihrer Integration an der Benutzeroberfläche von Kaspersky Next Expert View vornehmen.

Änderungen in der Benutzeroberfläche durch integrierte Kaspersky-Lösungen

Lösung	Änderungen in Kaspersky Next Expert View
Kaspersky EDR Optimum	Fügt die folgenden Elemente hinzu: • Abschnitt **Alarme** (**Überwachung** → **Alarme**). Die von dieser Lösung erkannten Alarme werden auf der Registerkarte **Optimum** angezeigt. • Ein Widget auf für das **Dashboard** (**Überwachung** → **Dashboard**).
Kaspersky MDR	Fügt die folgenden Elemente hinzu: • Den Abschnitt **MDR** (**Überwachung** → **MDR**). • Die Option **Funktionen von MDR anzeigen** (**Einstellungen** → **Einstellungen der Benutzeroberfläche** → **Funktionen von MDR anzeigen**). • Ein Widget auf für das **Dashboard** (**Überwachung** → **Dashboard**).
Kaspersky EDR Expert	Fügt die folgenden Elemente hinzu: • Abschnitt **Alarme** (**Überwachung** → **Alarme**). Die von dieser Lösung erkannten Alarme werden auf der Registerkarte **Expert** angezeigt. • Abschnitt **Vorfälle** (**Überwachung** → **Vorfälle**). • Abschnitt **Bedrohungssuche** (**Überwachung** → **Threat Hunting**). • Abschnitt **Benutzerdefinierte Regeln** (**Überwachung** → **Benutzerdefinierte Regeln**). • Allgemeine Einstellungen von Kaspersky EDR Expert (**Einstellungen** → **Integration** → **Kaspersky EDR Expert**). • Widgets für das **Dashboard** (**Überwachung** → **Dashboard**).

Data Discovery

Dieser Abschnitt enthält Informationen zu Data Discovery.

Über Data Discovery

Kaspersky Next Expert View erkennt kritische Informationen in Dateien, die sich in Cloud-Speichern von Microsoft 365 befinden. Sie können sich Informationen zu jeder gefundenen Datei ansehen: ihren Namen, den Typ ihrer Freigabe (privat, unternehmensintern oder unternehmensextern) und den Benutzer, der sie zuletzt bearbeitet hat.

Diese Funktion ist nur verfügbar, wenn Sie Kaspersky Next Expert View unter einer Lizenz für Kaspersky Next EDR Optimum oder XDR Expert aktiviert haben.

Um Data Discovery zu verwenden, aktivieren Sie die Funktion.

Das Data Discovery-Widget und die Tabelle zeigen Funde von kritischen Informationen in Dateien an. Das Widget zeigt bis zu 5 gefundene Dateien an und die Tabelle zeigt bis zu 1000 Funde an.

Aus der Tabelle von Data Discovery können Sie Informationen zu allen aktuellen Erkennungen in eine CVS-Datei exportieren.

Wenn Sie die Funktion nicht mehr verwenden möchten, können Sie diese deaktivieren. Sie können sie jederzeit wieder aktivieren.

Wenn Sie nach dem Starten der Verwendung von Data Discovery Ihren Arbeitsbereich löschen oder die Funktion deaktivieren und nicht erneut verwenden möchten, müssen Sie zu Microsoft 365 wechseln und die Berechtigungen, die Sie der Anwendung **Kaspersky App** erteilt haben, manuell widerrufen.

Kategorien der Informationen, die Data Discovery finden kann

Kaspersky Next erkennt kritische Informationen folgender Kategorien:

- Kredit-/Debitkartennummer
- Personenbezogene Daten aus Argentinien:
  - Argentinischer Führerschein
  - Argentinischer Personalausweis

    - Argentinischer Reisepass
    - Argentinische Steueridentifikationsnummer
- Personenbezogene Daten aus Brasilien:
    - Brasilianischer Führerschein (CNH)
    - Brasilianischer Personalausweis (RG)
    - Brasilianische Steuerregistrierung (CPF)
    - Brasilianischer Reisepass
- Personenbezogene Daten aus Chile:
    - Chilenischer Führerschein
    - Chilenischer Personalausweis
    - Chilenischer Reisepass
    - Chilenische Steueridentifikationsnummer
- Personenbezogene Daten aus Kolombien:
    - Kolumbianischer Führerschein
    - Kolumbianischer Personalausweis
    - Kolumbianischer Reisepass
    - Kolumbianische eindeutige Steuernummer (NIT)
- Personenbezogene Daten aus Ägypten:
    - Ägyptischer Führerschein
    - Ägyptischer Personalausweis
    - Ägyptischer Reisepass
- Personenbezogene Daten aus den Vereinigten Arabischen Emiraten:
    - Emiratischer Personalausweis (EID)
    - Emiratischer Reisepass
    - Emiratischer Führerschein
    - Emiratische einheitliche Nummer (UID)

- Personalausweis aus Frankreich
  - Französischer Führerschein
  - Französischer Personalausweis
  - Französischer Reisepass
  - Französische Sozialversicherungsnummer
- Personalausweis aus Deutschland
  - Deutscher Führerschein
  - Deutscher Personalausweis
  - Deutscher Reisepass
  - Deutsche Aufenthaltsgenehmigung
  - Deutsche Sozialversicherungsnummer (SVNR)
  - Deutsche steuerliche Identifikationsnummer (IdNr.)
- Personalausweis aus Indien
  - Indischer Führerschein
  - Indische Identifikationsnummer für Waren- und Dienstleistungssteuer
  - Indische Identifikationsnummer (Aadhaar)
  - Indischer Reisepass
  - Indische Steuer-Identifikationsnummer
  - Indischer Wählerausweis
- Personenbezogene Daten aus Italien:
  - Italienischer Führerschein
  - Italienische Steuernummer
  - Italienischer Personalausweis
  - Italienischer Reisepass
- Personenbezogene Daten aus Malaysia:
  - Malaysischer Führerschein
  - Malaysischer Personalausweis
  - Malaysische Steueridentifikationsnummer

- Personenbezogene Daten aus Mexiko:
  - Mexikanischer eindeutiger persönlicher Registrierungscode (CURP)
  - Mexikanische individuelle Steuerregistrierung (CPF)
  - Mexikanischer Reisepass
  - Mexikanische Sozialversicherungsnummer
- Personenbezogene Daten aus Peru:
  - Peruanischer Führerschein
  - Peruanischer Personalausweis (DNI)
  - Peruanische Aufenthaltsgenehmigung
  - Peruanische Steueridentifikationsnummer (RUC)
- Personenbezogene Daten aus Portugal:
  - Portugiesische Bürgerkarte (CC)
  - Portugiesischer Führerschein
  - Portugiesischer Reisepass
  - Portugiesische Sozialversicherungsnummer (NISS)
  - Portugiesische Steuernummer (NIF)
- Personenbezogene Daten aus Saudi-Arabien:
  - Saudi-arabischer Führerschein
  - Saudi-arabischer Personalausweis
  - Saudi-arabische Aufenthaltsgenehmigung
  - Saudischer Reisepass
- Personenbezogene Daten aus Südafrika:
  - Südafrikanischer Personalausweis
  - Südafrikanischer Reisepass
  - Südafrikanische Steuerreferenznummer
- Personenbezogene Daten aus Spanien:
  - Spanischer Personalausweis
  - Spanische Sozialversicherungsnummer (NSS)

    - Spanischer Reisepass
    - Spanische steuerliche Identifikationsnummer (NIF)
- Personenbezogene Daten aus der Türkei:
    - Türkischer Führerschein
    - Türkische Aufenthaltserlaubnis
    - Türkischer Personalausweis
    - Türkische Versicherungsnummer (4/a SSK)
    - Türkischer Reisepass
    - Türkische Steuer-Identifikationsnummer
- Britische persönlich identifizierbare Informationen (UK):
    - Britischer Führerschein (UK)
    - Britische Sozialversicherungsnummer (UK)
    - Britischer Reisepass (UK)
    - Britische Aufenthaltsgenehmigung (UK)
    - Britische steuerliche Identifikationsnummer (UTR) (UK)
- Personenbezogene Daten aus den USA:
    - US-amerikanischer Führerschein
    - US-amerikanische individuelle steuerliche Identifikationsnummer (ITIN)
    - US-amerikanischer Reisepass
    - US-amerikanische Sozialversicherungsnummer (SSN)

Data Discovery aktivieren

Die Aktivierung von Data Discovery umfasst die folgenden Schritte:

1. Die Bedingungen der Vereinbarung für Data Discovery akzeptieren.
2. Verbinden einer Microsoft 365-Organisation mit Ihrem Arbeitsbereich.

Sie können die Funktion später wieder deaktivieren, wenn Sie sie nicht mehr verwenden möchten.

Die Bedingungen der Vereinbarung für Data Discovery akzeptieren

So akzeptieren Sie die Bedingungen der Vereinbarung für Data Discovery:

1. Öffnen der Management-Konsole von Kaspersky Next Expert View
2. Führen Sie eine der folgenden Aktionen aus:

   - (Wenn das Widget **Erkennungen von Data Discovery** zum Dashboard hinzugefügt wurde) Klicken Sie im Abschnitt **Überwachung** → **Dashboard** unter **Erkennungen von Data Discovery** auf die Schaltfläche **Data Discovery aktivieren**.
   - Klicken Sie im Abschnitt **Dienste** → **Data Discovery** auf die Schaltfläche **Data Discovery aktivieren**.

   Das Fenster **Vereinbarung zu Data Discovery** erscheint.
3. Lesen Sie die Vereinbarung sorgfältig durch, aktivieren Sie das Kontrollkästchen unter dem Text der Vereinbarung und klicken Sie dann auf die Schaltfläche **Ich akzeptiere die Bedingungen**, wenn Sie mit diesen einverstanden sind.

   > Wenn Sie auf die Schaltfläche **Ich lehne ab** klicken, können Sie Data Discovery nicht nutzen.

   Die Vereinbarung zur Data Discovery wurde akzeptiert.

   Kaspersky Next Expert View fordert Sie auf, Ihre Microsoft 365-Organisation mit Ihrem Arbeitsbereich zu verbinden.

Verbinden einer Microsoft 365-Organisation mit Ihrem Arbeitsbereich

Sobald Sie die Nutzungsbedingungen der Vereinbarung für Data Discovery akzeptiert haben, fordert Kaspersky Next Expert View Sie auf, Ihre Microsoft 365-Organisation mit Ihrem Arbeitsbereich in Kaspersky Next Expert View zu verbinden, wie in diesem Abschnitt beschrieben.

Danach können Sie die Funde von Data Discovery in der Management-Konsole anzeigen.

So verbinden Sie eine Microsoft 365-Organisation mit Ihrem Arbeitsbereich:

1. Öffnen der Management-Konsole von Kaspersky Next Expert View

   Wenn Sie gerade die Bedingungen der Vereinbarung für Data Discovery akzeptiert haben, können Sie diesen Schritt überspringen.

2. Führen Sie eine der folgenden Aktionen aus:

   - (Wenn das Widget **Erkennungen von Data Discovery** zum Dashboard hinzugefügt wurde) Klicken Sie im Abschnitt **Überwachung → Dashboard** unter **Erkennungen von Data Discovery** auf die Schaltfläche **Microsoft 365-Organisation verbinden**.
   - Klicken Sie im Abschnitt **Dienste → Data Discovery** auf die Schaltfläche **Microsoft 365-Organisation verbinden**.

   Wenn Sie gerade die Bedingungen der Vereinbarung für Data Discovery akzeptiert haben, können Sie diesen Schritt überspringen.

3. Wenn sich das Fenster **Microsoft 365-Organisation verbinden** öffnet, klicken Sie auf die Schaltfläche **Verbinden**.

   Sie werden auf die Website von Microsoft Online umgeleitet.

4. Geben Sie das erforderliche Konto des Globalen Administrators von Microsoft 365 an und bestätigen Sie die Erteilung der angeforderten Berechtigungen.

   > Das Global-Administrator-Konto, das Sie angeben, muss zu derselben Microsoft 365-Organisation gehören, für die Sie die Informationen abrufen möchten. Beachten Sie, dass Kaspersky Next Expert View die Anmeldedaten des Global Administrators nicht speichert und nur die erlangte Zustimmung nutzt.

   Sie werden wieder zurück zur Management-Konsole von Kaspersky Next Expert View geleitet.

Nachdem die angegebenen Anmeldedaten überprüft und verifiziert wurden, wird ihre Microsoft 365-Organisation mit ihrem Arbeitsbereich in Kaspersky Next Expert View verbunden. Kaspersky Next Expert View startet die erste Untersuchung von Dateien, die sich in den Cloud-Speichern von Microsoft 365 befinden.

Nachdem die Untersuchung abgeschlossen ist, können Sie die Funde im Data Discovery-Widget und in der Tabelle anzeigen.

Anzeigen von Informationen über Funde von Data Discovery

Sie können Informationen über Funde von Data Discovery in einem Widget und einer Tabelle einsehen. Das Widget zeigt bis zu 5 gefundene Dateien an und die Tabelle zeigt bis zu 1000 Funde an.

Das Widget von Data Discovery

Um das Data Discovery-Widget anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen der Management-Konsole von Kaspersky Next Expert View
2. Wählen Sie den Abschnitt **Überwachung → Dashboard** aus.

3. Wenn das Widget **Erkennungen von Data Discovery** auf dem Dashboard nicht angezeigt wird, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Widget hinzufügen oder wiederherstellen**.

   b. Erweitern Sie die Gruppe **Andere** und klicken Sie anschließend auf das Widget **Erkennungen von Data Discovery**.

   c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

4. Falls Data Discovery deaktiviert ist, aktivieren Sie die Funktion.

   Das Data Discovery-Widget zeigt bis zu 5 gefundene Dateien an.

5. Um detaillierte Informationen über eine gefundene Datei anzuzeigen, klicken Sie auf eine beliebige Stelle in der Zeile mit der gewünschten Datei.

Das Widget zeigt die angeforderten Informationen an.

Aus dem Widget können Sie die Tabelle mit den Funden von Data Discovery aufrufen.

Die Tabelle von Data Discovery

Um die Tabelle mit den Funden von Data Discovery anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen der Management-Konsole von Kaspersky Next Expert View

2. Führen Sie eine der folgenden Aktionen aus:

   - (Wenn das Widget **Erkennungen von Data Discovery** zum Dashboard hinzugefügt wurde) Klicken Sie im Abschnitt **Überwachung → Dashboard** unter **Erkennungen von Data Discovery** auf den Link **Zur Liste mit den Erkennungen wechseln**.

   - Wählen Sie den Abschnitt **Dienste → Data Discovery** aus.

3. Falls Data Discovery deaktiviert ist, aktivieren Sie die Funktion.

   Die Tabelle zeigt bis zu 1000 gefundene Dateien an.

4. Sortieren und filtern Sie die angezeigten Datensätze, indem Sie auf eine Spalte klicken und die erforderlichen Werte auswählen:

   - **Zuletzt geändert am** – Der Zeitraum, in dem Dateien bearbeitet werden.

   - **Dateiname** – Namen der gefundenen Dateien.

   - **Datenkategorien**: Kategorien von kritischen Informationen, die in den Dateien gefunden werden.

   - **Zugriffstyp**: Zielgruppe, für die die Dateien freigegeben sind (privat, unternehmensintern, unternehmensextern).

- **Zuletzt bearbeitet von** – Benutzerkonten der Benutzer, die die gefundenen Dateien zuletzt bearbeitet haben.

- **Dienst** – Name des Microsoft 365-Dienstes, der die gefundenen Dateien speichert.

5. Um detaillierte Informationen über eine gefundene Datei anzuzeigen, klicken Sie auf eine beliebige Stelle in der Zeile mit der gewünschten Datei.

In der Tabelle werden die angeforderten Informationen angezeigt.

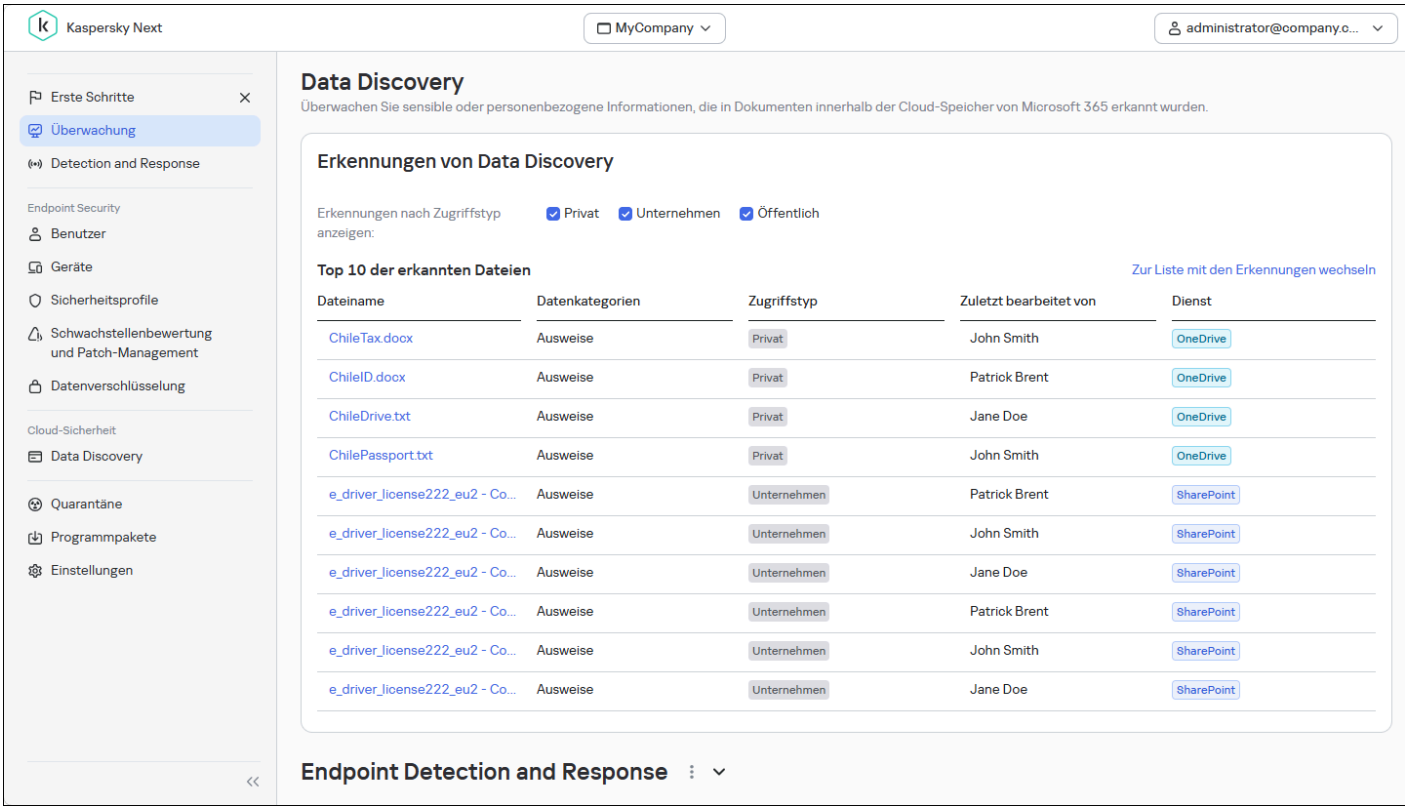
Aus der angezeigten Tabelle können Sie Informationen zu allen aktuellen Erkennungen in eine CVS-Datei exportieren.

In der angezeigten Tabelle können Sie auch auf die Schaltfläche **Einstellungen** klicken. Im angezeigten Fenster mit den **Einstellungen von Data Discovery** können Sie den Text der Vereinbarung für Data Discovery und die Liste der erfassten personenbezogenen Daten einsehen sowie Data Discovery deaktivieren.

Beispiel für die Analyse einer Erkennung von Data Discovery

Dieser Abschnitt enthält ein Beispiel für eine Erkennung von Data Discovery und wie Sie diese analysieren und verarbeiten können.

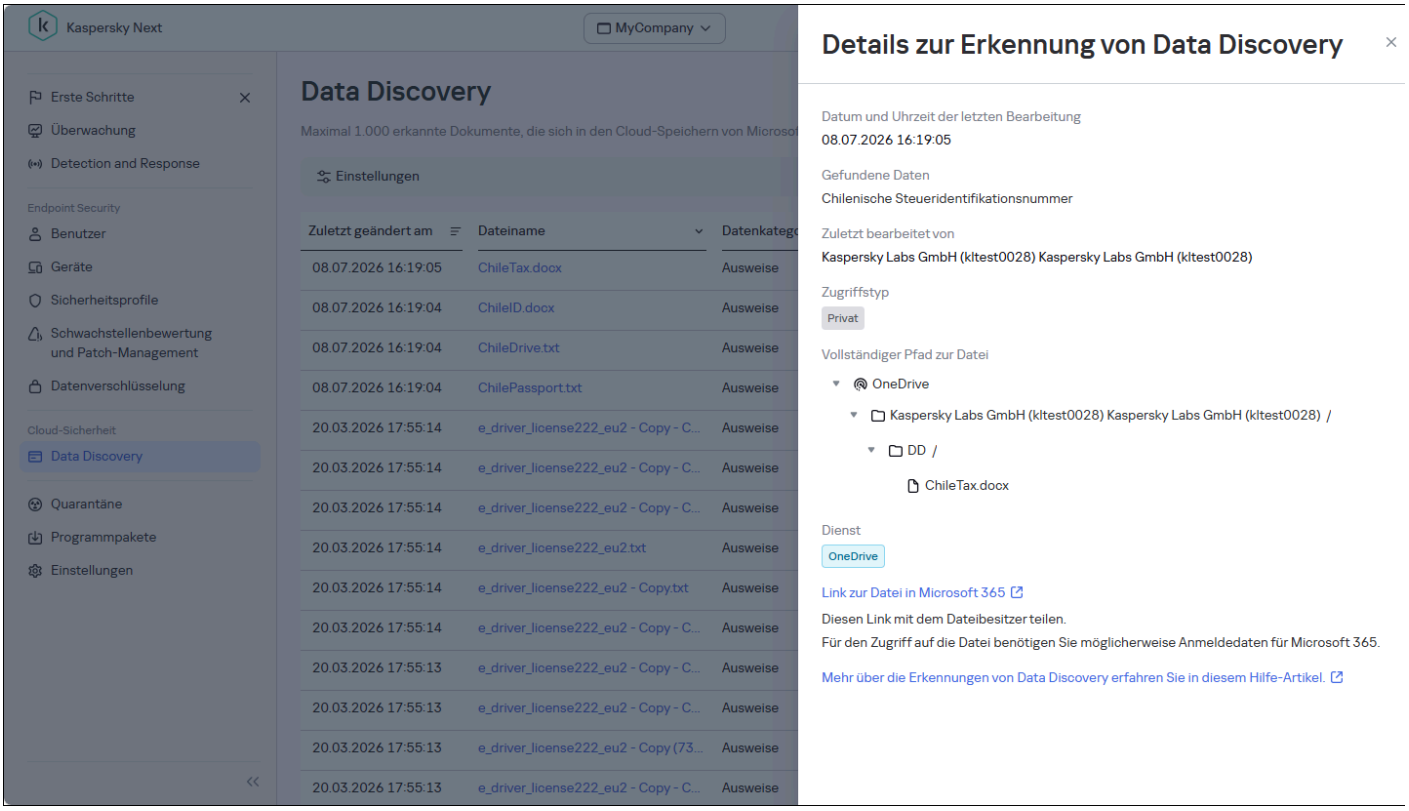
Angenommen, Sie öffnen das Widget von Data Discovery (siehe Abbildung unten) und sehen eine Datei, auf die jeder zugreifen kann (der Wert in der Spalte **Zugriffstyp** ist **Öffentlich**).



Das Widget von Data Discovery mit einer Datei, auf die jeder zugreifen kann

Aus dem Wert in der Spalte **Datenkategorien** schließen Sie, dass die Datei Kreditkartendaten enthält. Der Wert in der Spalte **Zuletzt bearbeitet von** zeigt in der Regel den Benutzer an, der die Zugriffseinstellungen der Datei konfiguriert hat.

Wenn Sie auf den Link in der Spalte **Dateiname** klicken, können Sie detaillierte Informationen zu der erkannten Datei anzeigen (siehe Abbildung unten).



Informationen zu den Erkennungen von Data Discovery

Sie können entweder den direkten Link zur Datei (**Link zur Datei in Microsoft 365**) oder ihre Pfadstruktur (unter **Vollständiger Pfad zur Datei**) kopieren.

Anschließend können Sie sich direkt an den Benutzer wenden, ihm die Datei zeigen und erklären, dass das Bereitstellen einer Datei mit persönlichen Daten für jedermann zu einer Datenverletzung führen kann. Sie können den Benutzer bitten, den Dateizugriff auf sich selbst zu beschränken.

Später, nachdem der Benutzer Ihrem Rat gefolgt ist, können Sie die Tabelle von Data Discovery öffnen, die Filter anwenden (falls erforderlich) und dasselbe Dokument anzeigen, das jetzt nur noch für seinen Eigentümer zugänglich ist (siehe Abbildung unten).

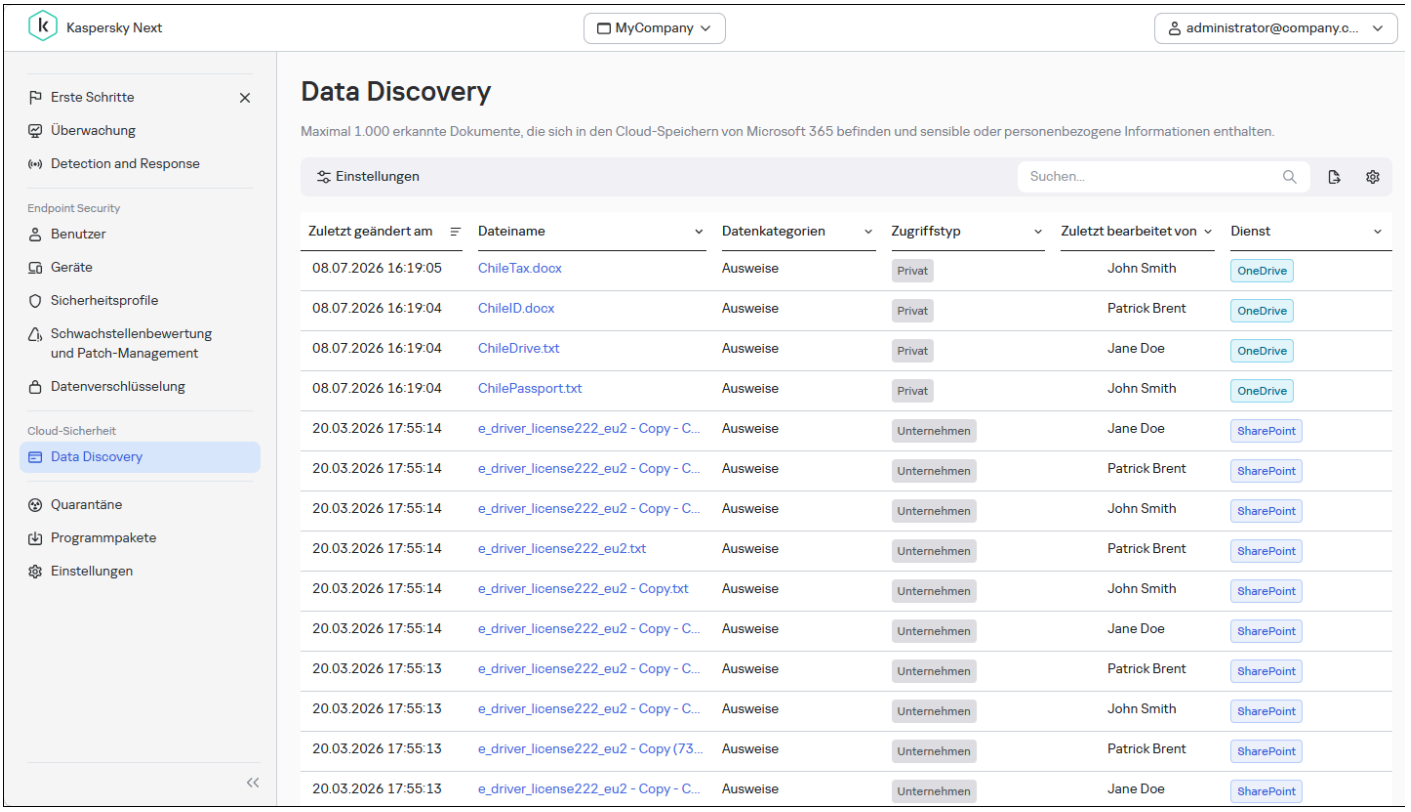


Tabelle von Data Discovery mit angewendeten Filtern

Informationen über Funde von Data Discovery exportieren

Sie können aus der Tabelle von Data Discovery Informationen zu allen aktuellen Erkennungen in eine CVS-Datei exportieren. Sie können beispielsweise eine Datei mit Funden verwenden, um einen Bericht für Ihr Management zu erstellen.

Exportieren von Informationen über Funde von Data Discovery:

1. Wechseln Sie zur Tabelle mit den Funden von Data Discovery.
2. Klicken Sie auf die Schaltfläche **Funde exportieren**.

   Das Fenster **Funde von Data Discovery exportieren** wird geöffnet.
3. Klicken Sie auf **Export**, um den Export zu bestätigen.

Es wird eine Datei mit den Funden von Data Discovery erstellt und automatisch heruntergeladen. Die Datei enthält dieselben Spalten wie die Tabelle der Funde.

Data Discovery deaktivieren

Wenn Sie Data Discovery nicht mehr verwenden möchten, können Sie die Funktion wie in diesem Abschnitt beschrieben deaktivieren.

So deaktivieren Sie Data Discovery:

1. Öffnen der Management-Konsole von Kaspersky Next Expert View
2. Klicken Sie im Abschnitt **Dienste** → **Data Discovery** auf die Schaltfläche **Einstellungen**.
   Die Seite mit den **Einstellungen von Data Discovery** wird geöffnet.
3. Deaktivieren Sie den Umschalter **Data Discovery ist aktiviert**.
4. Klicken Sie dann im Bestätigungsfenster auf die Schaltfläche **Deaktivieren**.

Data Discovery ist deaktiviert.

Sie können die Funktion später jederzeit wieder aktivieren.

Geräte im Netzwerk suchen und Administrationsgruppen erstellen

Dieser Abschnitt beschreibt, wie Geräte im Netzwerk gesucht und gefunden werden, und wie für diese Geräte Administrationsgruppen erstellt werden.

Kaspersky Next Expert View 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 Next Expert View Administrationsservers und seiner sekundären Administrationsserver.
- Nicht zugeordnete Geräte, die vom Administrationsserver der Kaspersky Next Expert View und seiner sekundären Administrationsserver verwaltet werden.

Szenario: Suche nach Netzwerkgeräten

Die Gerätesuche muss vor der erstmaligen Bereitstellung einer Sicherheitsanwendung ausgeführt werden. Sobald alle Geräte im Netzwerk gefunden wurden, können Sie Informationen zu diesen Geräten abrufen und sie mithilfe von Richtlinien verwalten. Regelmäßige Netzwerkabfragen sind nötig, um neue Geräte im Netzwerk zu erkennen und zu prüfen, ob sich die bereits erkannten Geräte noch im Netzwerk befinden.

Wenn Sie das Szenario abschließen, wird die Gerätesuche eingerichtet und nach dem angegebenen Zeitplan durchgeführt.

Erforderliche Vorrausetzungen

In Kaspersky Next Expert View wird die Gerätesuche mittels Verteilungspunkten durchgeführt. Führen Sie vor dem Start Folgendes durch:

- Legen Sie fest, welche Geräte als Verteilungspunkte fungieren sollen.
- Installieren Sie die Administrationsagenten auf den von Ihnen ausgewählten Geräten.
- Weisen Sie die Geräte manuell als Verteilungspunkte zu.

Schritte

Das Szenario verläuft in den folgenden Schritten:

1. **Auswählen der Art der Suche**

   Bestimmen Sie, welche Art(en) der Suche Sie regelmäßig verwenden möchten.

2. **Konfigurieren von Abfragen**

   Aktivieren und konfigurieren Sie in den Eigenschaften der einzelnen Verteilungspunkte die Arten der Netzwerkabfrage, die Sie ausgewählt haben: Windows-Netzwerkabfrage, Abfrage des Domänencontrollers oder IP-Bereichsabfrage. Stellen Sie sicher, dass der Abfragezeitplan den Anforderungen Ihres Unternehmens entspricht.

   Wenn Netzwerkgeräte zu einer Domäne gehören, wird es empfohlen, die Abfrage des Domänencontrollers zu verwenden.

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. Bei Bedarf können Sie die Regeln so konfigurieren, dass ein automatisches Verschieben dieser Geräte in die Gruppe **Verwaltete Geräte** stattfindet. Darüber hinaus können Sie Aufbewahrungsregeln einrichten.

   Wenn Sie diesen Schritt der Regelerstellung überspringen, werden alle neu entdeckten Geräte zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt und verbleiben dort. 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 die entsprechende Gruppe wählen.

Wenn eine Netzwerkabfrage abgeschlossen ist, überprüfen Sie, ob die neu entdeckten Geräte gemäß den konfigurierten Regeln zugeordnet wurden. (Falls keine Regeln konfiguriert sind, verbleiben die Geräte in der Gruppe **Nicht zugeordnete Geräte**).

Netzwerkabfrage

Informationen über die Struktur des Netzwerks und der Geräte in diesem Netzwerk erhält Kaspersky Next Expert View durch regelmäßiges Abfragen des Windows-Netzwerks, der IP-Bereiche, des Microsoft Active Directory-Domänencontrollers und des Samba-Domänencontrollers. Für einen Samba-Domänencontroller wird Samba 4 als Active Directory-Domänencontroller verwendet. Die Netzwerkabfrage kann entweder manuell oder automatisch nach einem Zeitplan gestartet werden.

Basierend auf den Ergebnissen dieser Abfrage aktualisiert Kaspersky Next Expert View die Liste der nicht zugeordneten Geräte. Sie können auch Regeln für neu erkannte Geräte konfigurieren, die automatisch in Administrationsgruppen verschoben werden sollen.

Kaspersky Next Expert View verwendet die folgenden Methoden zur Netzwerkabfrage:

- *IP-Bereiche durchsuchen*. Kaspersky Next Expert View fragt die angegebenen IP-Bereiche mit ICMP-Paketen (Internet Control Message Protocol) ab und erstellt einen vollständigen Datensatz mit den Geräten, die zu diesen IP-Bereichen gehören.

- *Windows-Netzwerkabfrage*. Sie können eine der beiden Windows-Netzwerkabfragen ausführen: schnell oder vollständig. Bei der Schnellabfrage empfängt Kaspersky Next Expert View nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks. Während einer vollständigen Abfrage werden die folgenden Informationen von jedem Gerät abgefragt: Name des Betriebssystems, IP-Adresse, DNS-Name und NetBIOS-Name.

- *Abfrage des Domänencontrollers*. Informationen über Struktur der Active Directory-Einheit und zu den DNS-Namen der Geräte aus Active Directory-Gruppen werden in der Datenbank von Kaspersky Next Expert View gespeichert.

Die Abfrageergebnisse werden im Abschnitt **Gerätesuche und Bereitstellung** → **Gerätesuche** für die Methoden *Windows-Netzwerkabfrage* und *Abfrage des Domänencontrollers* separat angezeigt.

Die Abfrageergebnisse für die Methode zur *Abfrage der IP-Bereiche* werden im Abschnitt **Gerätesuche und Bereitstellung** → **Nicht zugeordnete Geräte** angezeigt.

Ein Gerät kann in mehr als einem Erkennungsbereich angezeigt werden. Wenn ein Gerät in der HQ-Domäne erkannt wird und dessen Adresse "192.168.0.1" lautet, wird das Gerät sowohl im Abschnitt **Windows-Domänen** als auch im Abschnitt **Nicht zugeordnete Geräte** angezeigt. Sie können die Netzwerkabfrageeinstellungen für jede Abfragemethode separat ändern. Zum Beispiel können Sie den Abfragezeitplan ändern, oder definieren, ob die gesamte Active Directory-Struktur oder nur eine bestimme Domäne abgefragt werden soll.

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 müssen im Netzwerk verfügbar sein.

- Der Microsoft-Computersuchdienst muss verwendet werden, und der Computer mit dem primären Dienst muss auf dem Verteilungspunkt 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. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   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, den Sie zum Abfragen des Netzwerks verwenden möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Wählen Sie den Bereich **Abfrage der Windows-Domänen** aus.

5. Aktivieren oder deaktivieren Sie die Windows-Netzwerkabfrage mit dem Schalter **Netzwerkabfrage aktivieren**.

6. Konfigurieren Sie den Zeitplan für die schnelle und die vollständige Abfrage.

   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 am ausgewählten Tag**

     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.

7. Speichern Sie die Eigenschaften der Windows-Netzwerkabfrage.

Die Eigenschaften werden gespeichert und auf alle entdeckten Windows-Domänen und Arbeitsgruppen angewendet.

Abfrage des Domänencontrollers

Kaspersky Next Expert View unterstützt die Abfrage von Domänencontrollern nur unter Verwendung eines Verteilungspunkts. Für die folgenden Typen von Domänencontrollern können Sie Abfragen konfigurieren:

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

Kaspersky Next Expert View 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 ein Verteilungspunkt Informationen über die Domänenstruktur, Benutzerkonten, Sicherheitsgruppen und DNS-Namen jener Geräte ab, die zur Domäne gehören. Die Abfrage des Domänencontrollers erfolgt entsprechend eines Zeitplans den Sie vorher festgelegt haben.

Erforderliche Voraussetzungen

Stellen Sie vor der Abfrage eines Domänencontrollers sicher, dass die folgenden Protokolle aktiviert sind:

- Simple Authentication and Security Layer (SASL)
- Lightweight Directory Access Protocol (LDAP)

Stellen Sie sicher, dass die folgenden Ports auf dem Gerät des Domänencontrollers verfügbar sind:

- 389 für SASL
- 636 für TLS

Abfrage des Domänencontrollers mithilfe eines Verteilungspunkts

Sie können einen Domänencontroller auch mithilfe eines Verteilungspunkts abfragen. Als Verteilungspunkt kann ein verwaltetes Windows- oder Linux-Gerät fungieren.

Für einen Linux-Verteilungspunkt wird die Abfrage aller Domänencontrollertypen unterstützt.
Für einen Windows-Verteilungspunkt wird nur die Abfrage eines Microsoft Active Directory-Domänencontrollers unterstützt.
Die Abfrage mithilfe eines Mac-Verteilungspunkts 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. Schalten Sie im Feld **Abfrage** den Umschalter in die Position **Aktiviert**.
4. Wenn Sie einen Linux-basierten Verteilungspunkt verwenden, wählen Sie den Typ des abzufragenden Domänencontrollers aus.
5. 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**
6. 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 Next Expert View verwendet werden.

Ergebnisse der Abfrage des Domänencontrollers anzeigen

So zeigen Sie die Ergebnisse der Abfrage des Domänencontrollers an:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche →Domänencontroller**.
   Die Liste mit gefundenen Organisationseinheiten wird angezeigt.
2. Wählen Sie eine Organisationseinheit und klicken Sie dann auf die Schaltfläche **Geräte**.
   Die Liste mit Geräten in der Organisationseinheit wird angezeigt.

Sie können diese Liste durchsuchen und die Ergebnisse filtern.

IP-Bereiche abfragen

Kaspersky Next Expert View versucht für jede Adresse aus dem festgelegten Bereich die umgekehrte Namensauflösung (Reverse Name Resolution) 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 Next Expert View-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. Wenn diese Zone nicht konfiguriert ist, ergibt die IP-Subnetzabfrage keine Ergebnisse. 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.

Ursprünglich erhält Kaspersky Next Expert View die IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts mit dem Verteilungspunkt, der für die Netzwerkabfrage verwendet wird. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Next Expert View das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Next Expert View fragt alle Adressen von 192.168.0.1 bis 192.168.0.254 ab.

Es wird nicht empfohlen, die Abfrage von IP-Bereichen zu verwenden, wenn Sie die Windows-Netzwerkabfrage und/oder die Abfrage des Active Directory verwenden.

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. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
   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, den Sie zum Abfragen des Netzwerks verwenden möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Wählen Sie den Bereich **IP-Bereiche abfragen** aus.

5. Aktivieren oder deaktivieren Sie die IP-Abfrage mit dem Schalter **Abfrage des Bereichs aktivieren**.

6. Passen Sie den Abfragezeitplan an. Standardmäßig wird die IP-Abfrage alle 420 Minuten (sieben Stunden) ausgeführt.

7. Fügen Sie bei Bedarf abzufragende IP-Bereiche hinzu oder ändern Sie diese.

   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.

8. Klicken Sie auf die Schaltfläche **OK**.

Die Eigenschaften werden gespeichert und auf alle IP-Bereiche angewendet.

Einen Samba-Domänencontroller konfigurieren

Kaspersky Next Expert View unterstützt einen Linux-Domänencontroller, der nur auf Samba 4 ausgeführt wird.

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 Next Expert View 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.

IP-Bereich hinzufügen und bearbeiten

Ursprünglich erhält Kaspersky Next Expert View die IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts mit dem Verteilungspunkt, der für die Netzwerkabfrage verwendet wird. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Next Expert View das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Next Expert View 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.

Um einen neuen IP-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   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, den Sie zum Abfragen des Netzwerks verwenden möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Wählen Sie den Bereich **IP-Bereiche abfragen** aus.

5. Klicken Sie auf **Hinzufügen**, um den neuen IP-Bereich hinzuzufügen.

6. Passen Sie im nächsten Fenster folgende Einstellungen an:

   - **Name**

     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 beliebig viele Subnetze hinzufügen. Benannte IP-Bereiche dürfen sich nicht überlappen, aber für unbenannte Subnetze innerhalb eines IP-Bereichs gilt keine derartige Beschränkung.

   - **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.

7. Klicken Sie auf die Schaltfläche **OK**.

Der neue IP-Bereich wird zur Liste mit IP-Bereichen hinzugefügt.

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.

Verteilungspunkte und Verbindungs-Gateways anpassen

Die Struktur der Administrationsgruppen in Kaspersky Next Expert View 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 mithilfe von Tags, des Speicherorts der Geräte in den Active Directory-Verzeichnissen, der Zugehörigkeit zu den Sicherheitsgruppen Active Directory und anderen 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.

- Zugriffsrechte auf die Geräte und die sekundären Administrationsserver festlegen

- 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.

Anzahl und Konfiguration der Verteilungspunkte bestimmen

Je mehr Client-Geräte ein Netzwerk enthält, desto mehr Verteilungspunkte sind erforderlich. Anhand der folgenden Tabellen können Sie die Anzahl der für Ihr Netzwerk benötigten Verteilungspunkte berechnen.

Überzeugen Sie sich davon, dass die Geräte, die Sie als Verteilungspunkte verwenden 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 kein Verteilungspunkt verfügbar ist, aktualisieren Sie die Kaspersky-Datenbanken, Programm-Module und Programme manuell oder direkt über die Kaspersky-Update-Server.

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:

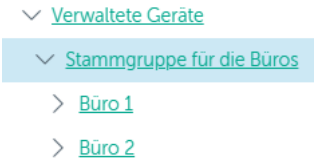
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen.

- Aufbau der Struktur der Administrationsgruppen, in der die Netztopologie nicht widergespiegelt wird. In diesem Fall müssen Sie 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.

Verteilungspunkte manuell zuweisen

In Kaspersky Next Expert View haben Sie die Möglichkeit, Geräte manuell zu Verteilungspunkten zu bestimmen. Es wird empfohlen, die Anzahl und Konfiguration der für Ihr Netzwerk benötigten Verteilungspunkte zu berechnen.

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.

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 auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Klicken Sie auf die Schaltfläche **Zuweisen**.

4. 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.

5. Wählen Sie die Administrationsgruppe aus, die zum Gültigkeitsbereich des ausgewählten Verteilungspunkts gehören soll.

6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Verteilungspunkt wird in der Liste der Verteilungspunkte im Abschnitt **Verteilungspunkte** angezeigt.

7. Wählen Sie den hinzugefügten Verteilungspunkt in der Liste aus und öffnen Sie sein Eigenschaftenfenster.

8. 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.

     - **Aktiviert**

       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 Next Expert View automatisch eine eindeutige IP-Multicasting-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 der Remote-Geräte**

  Die Netzwerkadresse, über die Remote-Geräte eine Verbindung zum Verteilungspunkt herstellen.

- **Aktiviert**

  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.

- **Aktiviert**

  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.

- **Aktiviert**

  In Kaspersky Next Expert View kann ein Verteilungspunkt als Push-Server für Windows-basierte und Linux-basierte Geräte fungieren, die durch einen Administrationsagenten verwaltet werden. 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 auf jedem der Verteilungspunkte einen Push-Server 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 Netzwerkstandort).

  Wenn Sie eine Administrationsgruppe angeben möchten, klicken Sie auf die Schaltfläche **Gruppe hinzufügen**. Wählen Sie im neuen rechten Bereich die Administrationsgruppe aus der Dropdown-Liste und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

  Wenn Sie ein Subnetz angeben möchten, klicken Sie auf die Schaltfläche **Subnetz hinzufügen**. Klicken Sie im neuen rechten Bereich auf die Schaltfläche **Hinzufügen** und geben Sie anschließend den Namen des Subnetzes ein.

  Für Geräte mit Windows-Betriebssystem wird der Umschalter **Verteilungspunkte mit dieser Beschreibung des Netzwerkstandorts automatisch zuweisen** angezeigt. Die Bestimmung des Netzwerkspeicherorts ist für Geräte unter der Verwaltung anderer Betriebssysteme nicht verfügbar.

- Im Abschnitt **Update-Quelle** können Sie eine Update-Quelle für den Verteilungspunkt auswählen:

- Wenn Ihre Verteilungspunkte für die Verbindung mit dem Internet einen Proxyserver verwenden, können Sie im Abschnitt **Einstellungen für die Internetverbindung** die folgenden Einstellungen festlegen:

  - **Proxyserver verwenden**

    Wenn dieses Kontrollkästchen aktiviert ist, wird ein Internet-Proxyserver verwendet, um die Verteilungspunkte mit den Kaspersky-Update-Servern zu verbinden. In den Eingabefeldern können Sie die Verbindung zum Proxyserver konfigurieren.

    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.

    > Diese Funktion wird von Verteilungspunktgeräten unter Linux- oder macOS nicht unterstützt.

    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 die Option **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** im Fenster mit den Eigenschaften des Administrationsservers aktiviert ist.

    Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

  - **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.

  - **HTTPS verwenden**

    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.

- **HTTPS-Port**

  Die Nummer des HTTPS-Ports, den die verwalteten Geräte verwenden sollen, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Der standardmäßige HTTPS-Port für die Verbindung zum KSN-Proxyserver ist 17111.

- Im Abschnitt **Verbindungs-Gateway** können Sie den Verteilungspunkt so konfigurieren, dass er als Gateway für die Verbindung zwischen den Instanzen der Administrationsagenten und dem Administrationsserver dient, wenn aufgrund der Organisation Ihres Netzwerks keine direkte Verbindung hergestellt werden kann. Aktivieren Sie dazu den Umschalter **Verbindungs-Gateway**.

  Diese Option ist standardmäßig deaktiviert.

  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 Domänencontrollers oder des IP-Bereichs für den Verteilungspunkt an:

  - **Abfrage der Windows-Domänen**

    Sie können die Geräteerkennung für Windows-Domänen aktivieren, indem Sie den Umschalter **Netzwerkabfrage aktivieren** aktivieren und anschließend auf die Schaltfläche **Zeitplan für vollständige Abfragen festlegen** klicken, um den Zeitplan für die Erkennung festzulegen.

    Geben Sie im nächsten Fenster den Abfragezeitplan an:

    - **Start nach Zeitplan**

Sie können eine der folgenden Varianten für den Zeitplan auswählen:

- **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 am ausgewählten Tag**

  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.

- **Startintervall (Tage)**

  Geben Sie an, wofür n steht (Minuten oder Tage).

  Das Feld wird angezeigt, wenn Sie für den Zeitplan die Option **Alle n Tage** oder **Alle n Minuten** ausgewählt haben.

- **Beginnend ab**

  Geben Sie an, wann mit der ersten Abfrage begonnen werden soll.

  Das Feld wird angezeigt, wenn Sie für den Zeitplan die Option **Alle n Tage** oder **Alle n Minuten** ausgewählt haben.

- **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.

  Diese Option ist standardmäßig deaktiviert, weshalb der Administrationsserver auf den nächsten für die Abfrage geplanten Zeitpunkt wartet.

  Wenn Sie diese Option aktivieren, startet der Administrationsserver die Abfrage sofort, nachdem er eingeschaltet wurde.

Dieser Abschnitt wird nur für Verteilungspunkte mit Windows angezeigt.

- **Abfrage des Domänencontrollers**

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.

Nachdem Sie im Feld **Abfrage** die Taste auf **Aktiviert** gewechselt haben, können Sie Domänencontroller für die Abfrage auswählen und den Abfragezeitplan für diese 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. Außerdem können Sie den Typ der abzufragenden Domäne angeben: Active Directory oder Samba, FreeIPA, ALD Pro.

Wenn Sie einen Windows-Verteilungspunkt verwenden, können Sie eine der folgenden Optionen auswählen:

- **Aktuelle Domäne abfragen**
- **Domänengesamtstruktur abfragen**
- **Angegebene Domänen abfragen**

- **IP-Bereiche abfragen**

  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.

- **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.

- Im Abschnitt **Statistik** können Sie Statistiken zum Download von Antiviren-Datenbanken oder zur Installation von Paketen auf dem Gerät anzeigen.

9. 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. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.

2. Eine Administrationsgruppe, für die Sie die zugewiesenen Verteilungspunkte anzeigen wollen, wählen Sie aus, indem Sie im oberen Bereich der Seite auf **Hierarchie anzeigen** klicken und anschließend im neuen Fenster den Namen der erforderlichen Gruppe anklicken.

   Dadurch wird die Anzeige des Menüpunkts **Verteilungspunkte** aktiviert.

   Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie innerhalb dieses Pfades auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv.

3. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Verteilungspunkte**.

4. Fügen Sie mithilfe der Schaltfläche **Zuweisen** neue Verteilungspunkte zur Administrationsgruppe hinzu oder löschen Sie zugewiesene Verteilungspunkte mithilfe der Schaltfläche **Zuweisen aufheben**.

   > Nachdem Sie auf die Schaltfläche **Zuweisen aufheben** geklickt haben, wird das Gerät nicht nur aus der Administrationsgruppe entfernt, sondern agiert auch nicht mehr als Verteilungspunkt.

Je nach Ihren Änderungen werden neue Verteilungspunkte zur Liste hinzugefügt oder bestehende Verteilungspunkte daraus entfernt.

Verteilungspunkt als Push-Server verwenden

In Kaspersky Next Expert View kann ein Verteilungspunkt als Push-Server für Windows-basierte und Linux-basierte Geräte fungieren, die durch einen Administrationsagenten verwaltet werden. 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 auf jedem der Verteilungspunkte einen Push-Server aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

Sie können Verteilungspunkte als Push-Server verwenden, um sicherzustellen, dass eine dauerhafte 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 ein verwaltetes Programm oder die Herstellung eines Tunnels. Wenn Sie einen Verteilungspunkt als Push-Server verwenden, müssen Sie keine Pakete an den UDP-Port des Administrationsagenten senden.

So verwenden Sie einen Verteilungspunkt als Push-Server:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Klicken Sie auf den Verteilungspunkt, den Sie als Push-Server verwenden möchten.

4. Gehen Sie in den Eigenschaften des ausgewählten Push-Servers zum Abschnitt **Allgemein** und aktivieren Sie anschließend die Option **Aktiviert**.

   Das Eingabefeld **Port des Push-Servers** wird verfügbar.

5. Geben Sie im Eingabefeld **Port des Push-Servers** Port des Verteilungspunkts an, den die Client-Geräte für die Verbindung verwenden. Standardmäßig ist die Portnummer 13295 festgelegt.

   > In den Firewall-Regeln müssen Sie ausgehende Netzwerkverbindungen zwischen den verwalteten Geräten und dem Port des Push-Servers zulassen.

6. Klicken Sie auf **OK**, um das Eigenschaftenfenster des Verteilungspunkts zu verlassen, und klicken Sie anschließend auf **Speichern**, um die Änderungen zu übernehmen.

   Nachdem Sie die Option **Aktiviert** aktiviert haben, wird die Option **Verbindung mit Administrationsserver nicht trennen** automatisch auf dem Verteilungspunkt aktiviert, der als Push-Server fungiert. Diese Option ermöglicht eine frühzeitige Verbindung zwischen dem Administrationsagenten und dem Administrationsserver.

7. Öffnen Sie das Fenster mit den Eigenschaften des Administrationsagenten.

8. Gehen Sie zu **Konnektivität** → **Netzwerk** und aktivieren Sie anschließend die Option **Verteilungspunkt verwenden, um eine Verbindung zum Administrationsserver zu erzwingen**. Schließen Sie das Schloss für diese Option.

9. Im Unterabschnitt **Netzwerk** können Sie auch die Option **UDP-Port verwenden** deaktivieren. Der konfigurierte Push-Server stellt eine dauerhafte Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver her, anstatt Pakete über den UDP-Port zu senden.

10. 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.

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 Next Expert View 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. Führen Sie eine der folgenden Aktionen aus:

   - Wenn das verwaltete Gerät auf direkt auf den Administrationsserver zugreift (d. h. nicht via Verteilungspunkt), gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)** und klicken Sie anschließend auf den Namen des Geräts, mit dem Sie eine dauerhafte Verbindung herstellen möchten.

     Das Eigenschaftenfenster des verwalteten Geräts wird geöffnet.

   - Wenn das verwaltete Gerät nicht direkt, sondern über einen Verteilungspunkt im Gateway-Modus auf den Administrationsserver zugreift:

     a. Öffnen Sie das Eigenschaftsfenster des Administrationsservers, indem Sie im Hauptmenü auf den Namen des Administrationsservers klicken.

     Alternativ dazu können Sie die Eigenschaften des erforderlichen Administrationsservers über den Navigationsbereich aufrufen. Wählen Sie dazu im Hauptmenü einen beliebigen Abschnitt (außer **Marketplace**, **Konsolen-Navigation** und **Einstellungen**) und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen des gewünschten Administrationsservers und klicken Sie anschließend auf das Einstellungssymbol (⚙).

     b. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

c. Klicken Sie in der Liste mit Verteilungspunkten auf den Namen des benötigten Verteilungspunkts.

Das Eigenschaftenfenster des ausgewählten Verteilungspunkts wird geöffnet.

2. Wählen Sie im Abschnitt **Allgemein** des geöffneten Eigenschaftenfensters 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.

Administrationsgruppen anlegen

Die Hierarchie der Administrationsgruppen enthält zunächst nur eine Administrationsgruppe namens **Verwaltete Geräte**. Wenn Sie eine Hierarchie der Administrationsgruppen erstellen, können Sie Geräte und virtuelle Maschinen zur Gruppe **Verwaltete Geräte** und zu untergeordneten Gruppen hinzufügen. Für jede Administrationsgruppe enthält das Eigenschaftenfenster Informationen über Richtlinien, Aufgaben und Geräte, die sich auf die Gruppe beziehen.

Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Aktivieren Sie das Kontrollkästchen neben der Administrationsgruppe, für die Sie eine neue Untergruppe anlegen möchten.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.
4. Geben Sie einen Namen für die neue Administrationsgruppe ein.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

In der Hierarchie der Administrationsgruppen erscheint eine neue Administrationsgruppe mit dem angegebenen Namen.

Das Programm ermöglicht es, 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 **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Klicken Sie auf die Schaltfläche **Importieren**.

Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Schritten des Assistenten.

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 **Asset-Verwaltung** → **Verschiebungsregeln**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**. Das Fenster **Neue Regel** wird geöffnet.
3. Geben Sie 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.

   - **Priorität**

     Sie können die Priorität der zu verschiebenden Regel festlegen. Der Wert "1" entspricht der höchsten Priorität. Je größer der **Priorität**, desto niedriger ist die Priorität der Regel und ihre Position in der Liste.

     Wenn keine Priorität zugewiesen ist, wird der Regel die niedrigste Priorität zugewiesen.

     Wenn eine Regel kopiert wird, wird der Kopie die Priorität der Originalregel zugewiesen. Die Priorität der Originalregel wird in diesem Fall um 1 erhöht.

   - **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.

So ändern Sie die Priorität:

1. Aktivieren Sie das Kontrollkästchen einer zu verschiebenden Regel.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf die Schaltfläche **Priorität ändern** und geben Sie anschließend die neue Priorität an.
   - Verschieben Sie die Regel in der Liste nach oben oder unten, indem Sie die entsprechenden Schaltflächen **Nach oben** oder **Nach unten** anklicken.
3. Klicken Sie auf die Schaltfläche **Speichern**.

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 **Asset-Verwaltung** → **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.

   - **Priorität**

     Sie können die Priorität der zu verschiebenden Regel festlegen. Der Wert "1" entspricht der höchsten Priorität. Je größer der **Priorität**, desto niedriger ist die Priorität der Regel und ihre Position in der Liste.

     Wenn keine Priorität zugewiesen ist, wird der Regel die niedrigste Priorität zugewiesen.

     Wenn eine Regel kopiert wird, wird der Kopie die Priorität der Originalregel zugewiesen. Die Priorität der Originalregel wird in diesem Fall um 1 erhöht.

   - **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:

- **Gilt für Geräte ohne die angegebenen Tags**

  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 Next Expert View verwenden, die Unterscheidung zwischen Groß- und Kleinschreibung aktiviert 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 Anwendungen

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.

- **Anwendungen**

  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 16.2 Administrationsagent** oder **Kaspersky Security Center 16.2 Administrationsserver** angeben.

  Wenn Sie keine verwaltete Anwendung auswählen, trifft die Bedingung nicht zu.

- **Aktiviert**

  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.

- **Architektur des Betriebssystems**

  Sie können Client-Geräte anhand der Bitanzahl des Betriebssystems auswählen. Im Block **Architektur 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 **Asset-Verwaltung** → **Assets (Geräte)**.
  2. Klicken Sie auf die Schaltfläche **Tabelleneinstellungen** ( ) auf der rechten Seite.
  3. Aktivieren Sie die Option **Architektur des Betriebssystems** und klicken Sie anschließend auf die Schaltfläche **Speichern**.

     Danach wird die Bitanzahl des Betriebssystems für jedes verwaltete Gerät angezeigt.

- **Paketverwaltung des Betriebssystems**

  Sie können Client-Geräte über den Paketmanager des Betriebssystems auswählen. Im **Paketverwaltung des Betriebssystems**-Feld können Sie einen der folgenden Werte auswählen:

  - rpm – für Geräte, auf denen die Betriebssysteme Red Hat Enterprise Linux, CentOS, Fedora, SUSE und Oracle Linux laufen
  - apt (dpkg) – für Geräte, auf denen die Betriebssysteme Debian-, Ubuntu und Kali laufen
  - pkg – für Geräte, auf denen die Betriebssysteme FreeBSD und OpenBSD laufen

  So überprüfen Sie den Paketmanager des Betriebssystems der Client-Geräte:

  1. Gehen Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)**.
  2. Klicken Sie auf die Schaltfläche **Spalteneinstellungen** () auf der rechten Seite.
  3. Wählen Sie die **Paketverwaltung des Betriebssystems**-Option und klicken Sie dann auf die **Speichern**-Schaltfläche.

  Der Paketmanager des Betriebssystems wird 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.

- **Aktiviert**

  > 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.

- **Aktiviert**

  > 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 Verschiebungsregeln für Geräte für die Geräte aus der Active Directory-Organisationseinheit, die in der Liste unter der Option angegeben ist.

  Diese Option ist standardmäßig deaktiviert.

- **Untergeordnete Organisationseinheiten einschließen**

  Wenn die Option aktiviert ist, werden in die Auswahl Geräte aufgenommen, die zu einem Unterverzeichnis der angegebenen Active Directory-Organisationseinheit gehören.

  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 Domänen-Sicherheitsgruppe**

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregeln für Geräte für die Geräte aus der Active Directory-Gruppe, 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.

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 **Asset-Verwaltung → Assets (Geräte)**.
2. Wählen Sie die Administrationsgruppe aus, der Sie die Geräte hinzufügen möchten.

   - Für die Stammgruppe:

     In diesem Fall können Sie mit dem nächsten Schritt fortfahren.

   - Für eine untergeordnete Gruppe:

     Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen** und anschließend im neuen Fenster auf den Namen der Untergruppe.

     Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv. Außerdem können Sie das Hierarchiefenster schließen, indem Sie auf die Schaltfläche **Hierarchie verbergen** klicken.

3. Klicken Sie auf die Schaltfläche **Geräte hinzufügen**.

   Daraufhin wird der Assistent für das Verschieben von Geräten gestartet.

4. 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, keine Backspace-Zeichen sowie keine 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, keine Backspace-Zeichen, sowie keine der folgenden verbotenen Zeichen enthalten: , \ / * ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

5. Zeigen Sie die Liste der Geräte an, die der Administrationsgruppe hinzugefügt werden sollen. Sie können die Liste bearbeiten, indem Sie Geräte hinzufügen oder entfernen.

6. 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, navigieren Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)** und wählen Sie anschließend die gewünschte Administrationsgruppe aus.

     - Für die Stammgruppe können Sie mit dem nächsten Schritt fortfahren.

     - Klicken Sie für eine Untergruppe im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen** und wählen anschließend im neuen Fenster eine erforderliche Administrationsgruppe.

   - 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 **Assets (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.

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 Next Expert View ermöglicht die Abschreibung von Hardware. 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.

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

Stellen Sie vor dem Start sicher, dass Sie das Szenario zur Erstkonfiguration von Kaspersky Next Expert View einschließlich des Schnellstartassistenten ausgeführt haben.

Während der Ausführung des Schnellstartassistenten in der Administrationsgruppe für **Verwaltete Geräte** werden die folgenden Richtlinien und Aufgaben erstellt:

- Richtlinie von Kaspersky Endpoint Security
- Gruppenaufgabe zum Update von Kaspersky Endpoint Security
- Richtlinie für den Administrationsagenten
- Suche nach Schwachstellen und erforderlichen Updates (Aufgabe des Administrationsagenten)

Schritte

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 installierten Kaspersky-Anwendungen stehen zwei unterschiedliche Methoden der Sicherheitsverwaltung zur Auswahl: die geräteorientierte und die benutzerorientierte Methode. Sie können diese beiden Ansätze auch kombinieren.

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:

- Gruppenaufgabe für das Update von Kaspersky Endpoint Security einrichten
- Erstellen der Aufgabe *Find vulnerabilities and required 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: Die Beschränkung der maximalen Anzahl der Ereignisse einstellen.

4. **Auslastung der Anwendungen zum Endpunktschutz optimieren**

   Um Leistungseinbußen zu vermeiden, optimieren Sie den Ressourcenverbrauch durch die Anwendungen zum Endpunktschutz.

   Anleitungen dazu erhalten Sie hier:

   Hilfe zu Kaspersky Endpoint Security für Windows

   Hilfe zu Kaspersky Endpoint Security für Linux

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 Datenbanken und Anwendungen von Kaspersky fortfahren.

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 Anwendungseinstellungen auf verschiedene Geräte anzuwenden, können Sie eine dieser Verwaltungsmethoden oder eine Kombination aus beiden Methoden verwenden.

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.

Einrichtung und Verteilung von Richtlinien: geräteorientierte Herangehensweise

Dieser Abschnitt beschreibt das Szenario der geräteorientierten 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.

Sie können auch eine benutzerzentrierte Sicherheitsverwaltung als Alternative oder zusätzliche Option zum gerätezentrierten Ansatz in Betracht ziehen.

Prozess

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 Next Expert View eine Standardrichtlinie für Kaspersky Endpoint Security für Windows. 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 über eine hierarchische Struktur aus mehreren Administrationsgruppen verfügen, erben die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen 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 verbliebenen, 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. **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:

   - Richtlinienprofil erstellen
   - Regeln für die Aktivierung des Richtlinienprofils erstellen

3. **Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergeben**

   Kaspersky Next Expert View synchronisiert den Administrationsserver mehrmals pro Stunde automatisch mit den verwalteten Geräten. 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 Next Expert View registriert das Datum und die Uhrzeit der Weitergabe in den Eigenschaften des Geräts.

Anleitung: 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.

Sie sollten zusätzlich auch die geräteorientierte Sicherheitsverwaltung als Alternative oder als zusätzliche Option zur benutzerorientierten Herangehensweise in Betracht ziehen. Erfahren Sie mehr über die 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 Next Expert View 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 über eine hierarchische Struktur aus mehreren Administrationsgruppen verfügen, erben die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen 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 verbliebenen, 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 Programmfunktionen.

   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**

   Kaspersky Next Expert View synchronisiert den Administrationsserver mehrmals pro Stunde automatisch mit den verwalteten Geräten. 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 Next Expert View 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 **Asset-Verwaltung** → **Richtlinien**.
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.

Registerkarte Allgemein

Auf dieser Registerkarte können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:
  - **Aktiv**
  - **Inaktiv**

    Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.
- In der Einstellungsgruppe **Vererbung von Einstellungen** 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.

Registerkarte 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. 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.

Registerkarte Anwendungseinstellungen

Einstellungen

Im Abschnitt **Einstellungen** können Sie die Richtlinieneinstellungen des Administrationsagenten anpassen:

- **Dateien nur über Verteilungspunkte übertragen**

  Wenn diese Option aktiviert ist, empfangen Client-Geräte die Updates nur über Verteilungspunkte und nicht direkt von den Update-Servern.

  Wenn diese Option deaktiviert ist, können Client-Geräte die Updates aus verschiedenen Quellen empfangen: direkt von den Update-Servern, aus einem lokalen Ordner oder aus einem Netzwerkordner.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Ereigniswarteschlange (MB)**

- **Der Anwendung 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**.

  Beachten Sie, dass das Tool "klmover" nur zum Verschieben von verwalteten Geräten verwendet wird, die von einem virtuellen Administrationsserver verwaltet werden.

  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:

- **Informationen über installierte Anwendungen**
- **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 zu Schwachstellen in Programmen und entsprechenden Updates**

  Wenn diese Option aktiviert ist, werden Informationen über Schwachstellen in Drittherstellern-Anwendungen (Microsoft-Software eingeschlossen), die auf verwalteten Geräten erkannt wurden, sowie Informationen über Software-Updates zum Beheben der Drittherstellern-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 das Hardware-Register**

Software-Updates und Schwachstellen

Im Abschnitt **Software-Updates und Schwachstellen** können Sie die Suche von Windows-Updates anpassen sowie die Untersuchung von ausführbaren Dateien auf Schwachstellen aktivieren. Die Einstellungen im Abschnitt **Software-Updates und Schwachstellen** sind nur auf Geräten verfügbar, die unter Windows laufen:

- 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 deaktiviert.

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

In dem Abschnitt **Windows Desktopfreigabe** können Sie das Audit der Tätigkeiten des Administrators bei Desktopfreigabe auf einem Remote-Gerät des Benutzers aktivieren und konfigurieren. Die Einstellungen im Abschnitt **Windows Desktopfreigabe** sind nur auf Geräten verfügbar, die unter Windows laufen:

- **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 Next Expert View

  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 Änderungen 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: Aktivieren oder deaktivieren der Option **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**.

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 **Verbindung mit dem Administrationsserver** können Sie folgenden Einstellungen angeben:
  - **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.

  - **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 Verteilungspunkteinstellungen die Option **Aktiviert** ausgewählt haben. Andernfalls wird der Verteilungspunkt nicht als Push-Server fungieren.

Da im Unterabschnitt **Verbindungsprofile** keine neuen Elemente zur Liste **Verbindungsprofile des Administrationsservers** hinzugefügt werden können, ist die Schaltfläche **Hinzufügen** inaktiv. Die voreingestellten Verbindungsprofile können ebenfalls nicht geändert werden.

Im Unterabschnitt **Verbindungszeitplan** können Sie Zeitintervalle festlegen, in denen der Administrationsagent Daten auf den Administrationsserver übertragen soll:

- **Verbindung bei Bedarf herstellen**

- **Verbindung in den angegebenen Zeiträumen herstellen**

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. Die Abfrageeinstellungen sind nur auf Geräten verfügbar, die unter Windows laufen. Sie können die folgenden Optionen verwenden, um die Abfrage zu aktivieren und ihre Häufigkeit festzulegen:

- **Windows-Netzwerk**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt automatisch das Netzwerk ab und richtet sich dabei nach dem Zeitplan, der über die Links **Zeitplan für schnelle Abfragen festlegen** und **Zeitplan für vollständige Abfragen festlegen** eingerichtet wurde.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver das Netzwerk nicht ab.

  Diese Option ist standardmäßig deaktiviert.

- **IP-Bereiche**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt automatisch die IP-Bereiche ab und richtet sich dabei nach dem Zeitplan, der über den Link **Abfragezeitplan festlegen** eingerichtet wurde.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt keine IP-Bereiche ab.

  Diese Option ist standardmäßig deaktiviert.

- **Domänencontroller**

  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

Im Abschnitt **Netzwerk-Einstellungen für Verteilungspunkte** können Sie die Einstellungen für den Internetzugang festlegen:

- **Proxyserver verwenden**

  Wenn diese Option aktiviert ist, wird ein Internet-Proxyserver verwendet, um die Verteilungspunkte mit den Kaspersky-Update-Servern zu verbinden.

- **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 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.

  > Diese Funktion wird von Verteilungspunktgeräten unter Linux- oder macOS nicht unterstützt.

  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 die Option **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** im Fenster mit den Eigenschaften des Administrationsservers aktiviert ist.

  Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

- **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.

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie:

- Den Verlauf der Richtlinienrevisionen anzeigen und speichern.
- Einen Rollback auf eine Richtlinienrevision durchführen.
- Beschreibungen von Richtlinienrevisionen hinzufügen und bearbeiten.
- Richtlinienrevisionen vergleichen.

Vergleich der Richtlinieneinstellungen des Administrationsagenten nach Betriebssystemen

Die folgende Tabelle zeigt, welche Richtlinieneinstellungen des Administrationsagenten Sie 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	✓	✓ Mit Ausnahme des Kontrollkästchens **Deinstallationskennwort verwenden**.	✓ Mit Ausnahme des Kontrollkästchens **Deinstallationskennwort verwenden**.
Datenverwaltung	✓	✓ Die Option **Informationen über das Hardware-Register** ist verfügbar.	✓ Es sind folgende Optionen verfügbar: • **Informationen über installierte Anwendungen** • **Informationen über das Hardware-Register**
Software-Updates und Schwachstellen	✓	—	—
Verwaltung des Neustarts	✓	—	—
Windows Desktopfreigabe	✓	—	—
Verwaltung von Patches und Updates	✓	—	—
Konnektivität → Netzwerk	✓	✓ Mit Ausnahme des Kontrollkästchens **Ports des Administrationsagenten in der Windows-Firewall öffnen**.	✓ Mit Ausnahme des Kontrollkästchens **Ports des Administrationsagenten in der Windows-Firewall öffnen**.
Konnektivität → Verbindungszeitplan	✓	✓	✓

Richtlinienabschnitt	Windows	macOS	Linux
Netzwerkabfrage durch Verteilungspunkte	✓ Es sind folgende Optionen verfügbar: • **Windows-Netzwerk** • **IP-Bereiche** • **Domänencontroller** (Microsoft Active Directory)	—	✓ Es sind folgende Optionen verfügbar: • **IP-Bereiche** • **Domänencontroller** (Microsoft Active Directory, Samba als Active Directory)
Netzwerk-Einstellungen für Verteilungspunkte	✓	✓	✓
KSN-Proxy (Verteilungspunkte)	✓	—	✓

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 neuer Updates in die Datenverwaltung**, wenn das Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert ist.

Aufgaben

In diesem Abschnitt werden Aufgaben beschrieben, die von Kaspersky Next Expert View verwendet werden.

Über Aufgaben

Kaspersky Next Expert View 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 können auf dem Administrationsserver und auf Geräten ausgeführt werden.

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 Werkzeuge zur Verwaltung 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.

- *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 jedes Programm mehrere Gruppenaufgaben, globale Aufgaben oder lokale 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.

Ausführungsergebnisse von Aufgaben werden in dem Betriebssystem-Ereignisprotokoll eines jeden Geräts 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.

Erstellen einer Aufgabe

Sie können eine Aufgabe in der Aufgabenliste erstellen. Alternativ können Sie in der Liste **Assets (Geräte)** die gewünschten Geräte auswählen und anschließend eine neue Aufgabe erstellen, die den ausgewählten Geräten zugewiesen ist.

So erstellen Sie eine Aufgabe in der Aufgabenliste:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → 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:

Gehen Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.

Die Liste der verwalteten Geräte wird angezeigt.

1. 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.
2. Klicken Sie auf die Schaltfläche **Aufgabe ausführen** und wählen Sie anschließend **Neue Aufgabe erstellen** 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.
3. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Die Aufgabe wird für die ausgewählten Geräte erstellt.

Aufgabenliste anzeigen

Sie können die Liste der Aufgaben anzeigen, die in Kaspersky Next Expert View erstellt wurden.

Um die Liste der Aufgaben anzuzeigen:

Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Aufgaben**.

Die Aufgabenliste wird angezeigt. Die Aufgaben sind nach den Namen der Programme gruppiert, auf die sie sich beziehen. Beispiele: Die Aufgabe *Remote-Deinstallation einer Anwendung* 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**.

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 **Assets (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 **Asset-Verwaltung** → **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.

Eine Aufgabe für ausgewählte Geräte starten

Sie können mehrere Client-Geräte aus der Geräteliste auswählen und anschließend eine zuvor für diese erstellte Aufgabe starten. Auf diese Weise können Sie Aufgaben ausführen, die zuvor für eine bestimmte Geräteauswahl erstellt wurden.

Dadurch wird beim Starten der Aufgabe anstelle der Geräte, denen die Aufgabe ursprünglich zugewiesen war, die Liste mit den von Ihnen ausgewählten Geräten angewendet.

So starten Sie eine Aufgabe für ausgewählte Geräte:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**. Die Liste der verwalteten Geräte wird angezeigt.

   Wählen Sie in der Liste der verwalteten Geräte mithilfe der Kontrollkästchen jene Geräte aus, für die Sie die Aufgabe ausführen möchten. Sie können die Such- und Filterfunktionen verwenden, um die gewünschten Geräte zu finden.
2. Klicken Sie auf die Schaltfläche **Aufgabe ausführen** und wählen Sie anschließend **Bestehende Aufgabe anwenden** aus.

   Die Liste der vorhandenen Aufgaben wird angezeigt.
3. Die ausgewählten Geräte werden oberhalb der Aufgabenliste angezeigt. Bei Bedarf können Sie Geräte aus dieser Liste entfernen. Die Liste muss mindestens ein Gerät enthalten.

4. Wählen Sie die gewünschte Aufgabe aus der Liste aus. Sie können das Suchfeld oberhalb der Liste verwenden, um die gewünschte Aufgabe anhand des Namens zu finden. Es kann nur eine Aufgabe ausgewählt werden.

5. Klicken Sie auf **Aufgabe speichern und ausführen**.

Die ausgewählte Aufgabe wird sofort für die ausgewählten Geräte gestartet. Der konfigurierte Zeitplan für den Aufgabenstart wird dabei nicht geändert.

Allgemeine Einstellungen und Eigenschaften von Aufgaben

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.

- Geräte, denen die Aufgabe zugewiesen wird:
  - **Aufgabe einer Administrationsgruppe zuweisen**

    Die Aufgabe wird 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**

    Die Aufgabe wird einer Reihe von Geräten zugewiesen. Sie können die Geräte auf eine der folgenden Arten angeben:

    - Geben Sie die IP-Adresse, den NetBIOS-Namen oder den DNS-Namen des Gerätes an.
    - Geben Sie den IP-Bereich an.

      Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Vielleicht wollen Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.
    - Wählen Sie die vom Administrationsserver gefundenen Geräte, einschließlich der nicht zugeordneten Geräte, aus.

      Sie können diese Option beispielsweise für eine Aufgabe zur Installation des Administrationsagenten auf nicht zugeordneten Geräten verwenden.

- **Aufgabe einer Geräteauswahl zuweisen**

  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.

- 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.

- Neustart-Einstellungen des Betriebssystems:

  - **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 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.

- **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.

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.

- Zeitplaneinstellungen für Aufgaben:

Die Arten des Zeitplans können je nach Aufgabe variieren.

- **Einstellung Aufgabe starten:**
  - **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.

  - **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 am ausgewählten Tag**

    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 neuer Updates in die Datenverwaltung**

  Wenn neue Updates in die Datenverwaltungen der Verteilungspunkte heruntergeladen wurden, führt Kaspersky Next Expert View alle Aufgaben aus, die dies als Zeitplan eingestellt haben. Der Administrationsagent überprüft die Verfügbarkeit von Updates mittels regelmäßiger Synchronisation zwischen dem verwalteten Gerät und dem Administrationsserver (der sog. Herzschlag).

  Beispielsweise können Sie diesen Zeitplan für die Update-Aufgabe verwenden, die sich auf eine Sicherheitsanwendung wie Kaspersky Endpoint Security bezieht.

  Wenn der Administrationsagent auf einem verwalteten Gerät für 25 Stunden oder länger keine neuen Updates findet, führt Kaspersky Next Expert View auf diesem Gerät alle Aufgaben aus, die dies als Zeitplan eingestellt haben. Diese Aufgaben werden stündlich ausgeführt, bis neue Updates gefunden wurden. Kaspersky Next Expert View führt diese Aufgaben auch dann stündlich aus, wenn zwischen dem verwalteten Gerät und dem Verteilungspunkt, der die Updates in die Datenverwaltung herunterlädt, keine Verbindung besteht.

- **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. Dieser Parameter 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**.

Die Zeitplaneinstellungen **können von der lokalen Zeitzone des Gerätebetriebssystems abhängig sein**.

Korrelation zwischen der lokalen Zeitzone des Gerätebetriebssystems und dem Startzeitpunkt der Aufgabe

Aufgabenzeitplan	Verwendet lokale Zeit
Einmal	Nein
Alle n Minuten	Nein
Alle n Stunden	Nein
Alle n Tage	Ja
Nach Wochentagen	Ja
Monatlich	Ja
Monatlich am ausgewählten Tag	Ja
Nach dem Download neuer Updates in die Datenverwaltung	Anderer Auslöser zum Ausführen der Aufgabe (entspricht dem Namen des Zeitplans)
Beim Erkennen eines Virenangriffs	Anderer Auslöser für die Aufgabenausführung (entspricht dem Namen des Zeitplans)
Nach Abschluss einer anderen Aufgabe	Anderer Auslöser für die Aufgabenausführung (entspricht dem Namen des Zeitplans)
Sofort	Anderer Auslöser für die Aufgabenausführung (entspricht dem Namen des Zeitplans)
Manuell	Anderer Auslöser für die Aufgabenausführung (entspricht dem Namen des Zeitplans)

- **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.

- **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.

- Benachrichtigungen:

  - Block **Ereignisdaten speichern**:

    - **Alle Ereignisse speichern**

    - **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**

    - **Nur die Ergebnisse der Aufgabenausführung 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.

- **Nur über Fehler benachrichtigen**
- **Per E-Mail benachrichtigen**

- Einstellungen für den Gültigkeitsbereich
- **Ausschlüsse vom Bereich**

  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 Next Expert View 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 **Asset-Verwaltung** → **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 Next Expert View können Sie eine Aufgabe aus einer klt-Datei importieren. Die klt-Datei enthält die exportierte Aufgabe und deren Einstellungen.

Damit die Aufgabe einer Kaspersky-Anwendung korrekt importiert wird, müssen Sie das entsprechende Verwaltungs-Plug-in installieren.

Um eine Aufgabe zu importieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **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)**.

Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen

Kaspersky Next Expert View 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**.

Client-Geräte verwalten

Mit Kaspersky Next Expert View können Sie Client-Geräte verwalten, indem Sie:

- 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 **Asset-Verwaltung** → **Assets (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. Dieser Status beruht auf den Kriterien, die der Administrator für den Status des Antiviren-Schutzes und die Aktivität des Geräts im Netzwerk festlegt.

    - **Gerätebesitzer**

      Name des Gerätebesitzers. Sie können einen Benutzer als Gerätebesitzer zuweisen oder entfernen. Dazu dient der Link **Gerätebesitzer verwalten**.

    - **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 Next Expert View.

- **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.

- **Sitzungen**

  Dieser Abschnitt enthält eine Tabelle mit Informationen zu den Benutzern, die aktuell am Gerät angemeldet sind. Die Tabelle zeigt die folgende Daten in den entsprechenden Spalten an:

  - Benutzername
  - Name des SAM-Kontos
  - Benutzer-Principal-Name (UPN)
  - E-Mail-Adresse

  Um Informationen über die Sitzungen von Domänenbenutzern korrekt anzuzeigen, müssen Sie die Abfrage des Domänencontrollers verwenden.

- 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**

  - **Hersteller des Betriebssystems**

  - **Ordner des Betriebssystems**

  - **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.

  - **Deaktiviert**

- Im Abschnitt **Schutz** werden die folgenden Informationen über den Status des Antiviren-Schutzes auf dem Client-Gerät angezeigt:

  - **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 enthält den aktuellen Status des Echtzeitschutzes auf dem Client-Gerät.

    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 durch Anwendung 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 Next Expert View vorgegebenen Status abweichen.

- **Anwendungen**

  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 dem Fenster können Sie Folgendes tun:

  - Schwachstellen in Programmen auf diesem verwalteten Gerät ignorieren (in der Verwaltungskonsole oder in Kaspersky Next Expert View).
  - Liste mit Korrekturen anzeigen, die für die Schwachstelle empfohlen werden.
  - Programm-Updates manuell angeben, um eine Schwachstelle zu beheben (in der Verwaltungskonsole oder in Kaspersky Next Expert View).
  - 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.

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 Richtlinieneinstellungen 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 Next Expert View.

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 Next Expert View bietet eine große Zahl an *vordefinierten Auswahlen* an (z. B. **Geräte mit dem Status "Kritisch"**, **Der Schutz ist deaktiviert**, **Aktive Bedrohungen wurden 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 für eine Geräteauswahl anzeigen

Mit der Kaspersky Next Expert View können Sie die Liste mit Geräten einer Geräteauswahl anzeigen.

So zeigen Sie die Geräteliste aus der Geräteauswahl an:

1. Gehen Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **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 **Asset-Verwaltung** → **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 aufnehmen** 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 **Asset-Verwaltung** → **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 **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 in die Auswahl Geräte aufgenommen, die zu einem Unterverzeichnis der angegebenen Active Directory-Organisationseinheit gehören.

  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.

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 Anwendungen** 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 Anwendungen** 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.

- **Architektur 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 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-Nummer 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.

- **Größe des Arbeitsspeichers (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.

- **Größe des Arbeitsspeichers (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:

- **Anwendungsname**

  In dieser Dropdown-Liste können Sie einen Anwendungsnamen auswählen. Die Geräte, auf denen diese Anwendung installiert ist, werden in die Auswahl aufgenommen.

- **Anwendungsversion**

  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.

- **Anwendungsstatus**

  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 **Anwendungsname**, **Anwendungsversion** und **Anwendungsstatus** 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.

- **Anwendungs-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.

- **Gilt für Geräte ohne die angegebenen Tags**

  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 Kaspersky-Anwendungen

Im Unterabschnitt **Kaspersky-Anwendungen** können Sie die Kriterien für die Aufnahme von Geräten anhand der ausgewählten verwalteten Anwendung konfigurieren:

- **Anwendungsname**

  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.

- **Anwendungsversion**

  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 Programm-Module 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 Next Expert View verwaltet werden:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn sie über Kaspersky Next Expert View verwaltet werden.
  - **Nein**. Das Programm nimmt Geräte in die Auswahl auf, wenn sie nicht über Kaspersky Next Expert View 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**

  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*.

  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.

Der Unterabschnitt **Programmkomponenten** enthält die Liste mit Komponenten von den Anwendungen, für die in der Kaspersky Next Expert View entsprechende Verwaltungs-Plug-ins 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. Beachten Sie, dass auf die Benutzerliste ein Filter angewendet wird und die Liste interne Benutzer anzeigt. In die Suchergebnisse werden Geräte aufgenommen, an dessen Systemen sich zuletzt der ausgewählte Benutzer angemeldet hat.

- **Benutzer, der sich mindestens einmal am System angemeldet hat**

  Wenn diese Option aktiviert ist, können Sie das Benutzerkonto für die Konfiguration des Kriteriums auswählen. Beachten Sie, dass auf die Benutzerliste ein Filter angewendet wird und die Liste interne Benutzer anzeigt. In die Suchergebnisse werden Geräte aufgenommen, an dessen Systemen sich der angegebene Benutzer mindestens einmal angemeldet hat.

Geräteliste einer Geräteauswahl exportieren

Mit Kaspersky Next Expert View 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**.

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 **Asset-Verwaltung** → **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.

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 **Asset-Verwaltung** → **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 Next Expert View weist jedem verwalteten Gerät einen Status zu. Der jeweilige Status hängt davon ab, ob die vom Benutzer definierten Bedingungen erfüllt sind. Wenn einem Gerät einen Status zugewiesen wird, berücksichtigt Kaspersky Next Expert View in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk (siehe folgende Tabelle). Wenn Kaspersky Next Expert View ein Gerät im Netzwerk nicht innerhalb von zwei Stunden 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
Sicherheitsanwendung ist nicht 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 im Rahmen einer Untersuchungsaufgabe (beispielsweise der Aufgabe "Untersuchung auf Viren") 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 wurden 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 durch Anwendung bestimmt	Der Gerätestatus wird von der verwalteten Anwendung bestimmt.	• Umschalter 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 Next Expert View ermöglicht eine Konfiguration der automatischen Umschaltung des Status von Geräten in der Administrationsgruppe bei Erfüllung der festgelegten 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 Kaspersky Next Expert View einem Gerät einen Status zuweist, wird für bestimmte Bedingungen (siehe Spalte "Beschreibung der Bedingung") das Sichtbarkeits-Flag berücksichtigt. 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*.

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 **Asset-Verwaltung** → **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 **Bekommt den Status "Kritisch" zugewiesen, wenn folgende Bedingungen erfüllt sind** 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 **Asset-Verwaltung** → **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 **Bekommt den Status "Warnung" zugewiesen, wenn folgende Bedingungen erfüllt sind** 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*.

Administrationsserver für Client-Geräte wechseln

Mit der Aufgabe **Administrationsserver 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 Geräteverwaltung zwischen folgenden Administrationsservers wechseln:

- Primärer Administrationsserver und einer seiner virtuellen Administrationsserver
- Zwei virtuelle Administrationsserver des gleichen primären Administrationsservers

Um einen Administrationsserver, der die Client-Geräte verwaltet, zu wechseln, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **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** die folgenden Einstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Next Expert View** 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** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

5. Bestätigen Sie im nächsten Schritt, dass Sie den Bedingungen für das Wechseln des Administrationsservers für Client-Geräte zustimmen.

6. Wählen Sie im nächsten Schritt den Administrationsserver aus, den Sie für die Verwaltung der ausgewählten Geräte verwenden möchten.

7. Geben Sie im Schritt **Benutzerkonto für die Ausführung der Aufgabe auswählen** 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 dessen Namen die Aufgabe gestartet wird.

8. Wenn Sie auf der Seite **Erstellung der Aufgabe abschließen** die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die standardmäßigen Aufgabeneinstellungen ändern.

   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.
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.

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 einer Anwendung* 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 einer Anwendung* 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 einer Anwendung* wird auf diese Geräte nicht angewendet.

Die Werte des Attributs **Verwaltung erfolgt durch anderen Administrationsserver** werden 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:

- Anzeigen verwalteter Geräte
- Geräteauswahlen
- Verschiebungsregeln für Geräte
- Regeln für die automatische Tag-Zuweisung

Um das Attribut Verwaltung erfolgt durch anderen Administrationsserver zurückzusetzen:

1. Wechseln Sie im Hauptmenü der Kaspersky Next Expert View zu **Gerätesuche und Bereitstellung → Nicht zugeordnete Geräte**.
2. Wählen Sie das gewünschte Gerät aus und klicken Sie anschließend auf die Schaltfläche **Attribut "Verwaltung erfolgt durch anderen Administrationsserver" entfernen**.

Das Attribut **Verwaltung erfolgt durch anderen Administrationsserver** wird zurückgesetzt.

Verbindungsprofile des Administrationsservers erstellen

Um es mobilen Benutzern zu ermöglichen, die Methode für die Verbindung des Administrationsagenten mit dem Administrationsserver zu ändern, müssen Sie die Verbindungsprofile des Administrationsservers konfigurieren.

So erstellen Sie ein Verbindungsprofil:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** und führen Sie einen der folgenden Schritte aus:

   - Wenn Sie ein Verbindungsprofil für eine Gruppe von verwalteten Geräten erstellen möchten, klicken Sie auf **Richtlinien** und anschließend auf **Kaspersky Security Center Administrationsagent**.

   - Wenn Sie ein Verbindungsprofil für ein bestimmtes verwaltetes Gerät erstellen möchten, klicken Sie auf **Assets (Geräte)** und anschließend auf den Namen des Geräts. Wechseln Sie im neuen Fenster zur Registerkarte **Anwendungen** und klicken Sie auf **Kaspersky Security Center Administrationsagent**.

   Das Eigenschaftenfenster der Richtlinie des Administrationsagenten wird geöffnet.

2. Wechseln Sie zur Registerkarte **Anwendungseinstellungen** und anschließend zum Abschnitt **Konnektivität**.

3. Klicken Sie im Abschnitt **Verbindungsprofile** auf die Schaltfläche **Einstellungen**.

   Im Unterabschnitt **Verbindungsprofile des Administrationsservers** wird die Tabelle der Verbindungsprofile angezeigt.

   > Die Verbindungsprofile **Home-Administrationsserver** und **Autonomer Modus** können nicht angezeigt, geändert oder gelöscht werden.

4. Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im neuen Fenster den Namen des Profils an.

   > Der Name muss eindeutig sein. Sie können denselben Namen nicht für mehrere Profile verwenden.

5. Aktivieren Sie bei Bedarf die Kontrollkästchen in den folgenden Feldern:

   - **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**

   - **Proxyserver verwenden**.

     Wenn Sie diese Option auswählen, gehen Sie wie folgt vor:

     - Geben Sie die notwendigen Informationen in den Feldern **Adresse** und **Port** an.

     - Aktivieren Sie bei Bedarf das Kontrollkästchen **Authentifizierung am Proxyserver** und geben Sie den Benutzernamen und das Kennwort in die entsprechenden Felder ein.

6. Klicken Sie auf **Speichern**.

Das neue Profil wird in der Tabelle mit den Verbindungsprofilen angezeigt. Sie können es verwenden, wenn Sie die Einstellungen für den **Netzwerkstandort konfigurieren**.

Die Einstellungen des Netzwerkstandorts 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).

Sie können Verbindungsprofile bearbeiten und löschen.

So bearbeiten Sie ein Verbindungsprofil:

1. Klicken Sie in der Tabelle mit den Verbindungsprofilen auf den Namen des Verbindungsprofils, das Sie bearbeiten möchten.
2. Nehmen Sie alle erforderlichen Änderungen vor und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Die Änderungen werden auf das Verbindungsprofil angewendet.

So löschen Sie ein Verbindungsprofil:

1. Aktivieren Sie in der Tabelle mit den Verbindungsprofilen die Kontrollkästchen neben den Verbindungsprofilen, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche **Löschen**.

   Die ausgewählten Verbindungsprofile werden gelöscht.

Über Cluster und Server-Arrays

Die Kaspersky Next Expert View 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 **Assets (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 Next Expert View 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 **Asset-Verwaltung** → **Assets (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 Next Expert View 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.

Geräte-Tags

Kaspersky Next Expert View erlaubt es Ihnen, den Geräten Tags zuzuweisen. Ein *Tag* ist die Bezeichnung des Geräts, 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. Sie können die manuelle Markierung verwenden, wenn Sie ein einzelnes Gerät markieren möchten. Die automatische Zuweisung der Tags wird von Kaspersky Next Expert View entsprechend den festgelegten Regeln zur Zuweisung von Tags ausgeführt.

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. Wenn Ihr Netzwerk beispielsweise Geräte enthält, auf denen Windows, Linux und macOS ausgeführt werden, können Sie eine Regel einrichten, die allen Linux-basierten Geräten das Tag `[Linux]` zuweist. Dieses Tag kann anschließend beim Erstellen einer Geräteauswahl verwendet werden, die Sie dabei unterstützt, alle Linux-basierten Geräte auszuwählen 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 **Asset-Verwaltung** → **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 **Asset-Verwaltung** → **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 **Asset-Verwaltung** → **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 **Asset-Verwaltung** → **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 **Assets (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 **Asset-Verwaltung** → **Assets (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 manuell den Geräten zuweisen

So weisen Sie den Geräten Tags 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.

So weisen Sie mehreren Geräten ein Tag zu:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
2. Wählen Sie die Geräte aus, denen Sie ein Tag zuweisen möchten.
3. Klicken Sie auf **Tags** und wählen Sie anschließend in der Dropdown-Liste die Option **Zuweisen** aus.
4. Wählen Sie im neuen Fenster ein Tag aus der Dropdown-Liste aus.

   Bei Bedarf können Sie mehrere Tags auswählen.

   Außerdem können Sie können Folgendes tun:

   - Bearbeiten Sie den Namen eines Tags, indem Sie auf Symbol **Bearbeiten** (✎) klicken.

     Geben Sie den neuen Namen des Tags ein und klicken Sie anschließend auf die Schaltfläche **Speichern**.

     Beachten Sie, dass das Tag auch in der Liste der Geräte-Tags umbenannt wird.

- Löschen Sie ein Tag, indem Sie auf Symbol **Löschen** (🗑) klicken

  Klicken Sie im neuen Fenster auf **Löschen**.

  > Beachten Sie, dass das Tag auch vom Administrationsserver gelöscht wird.

5. Klicken Sie auf **Speichern**.

Die Tags wurden den ausgewählten Geräten zugewiesen. Sie können die zugewiesenen Tags entfernen.

Zugewiesene Tags von Geräten entfernen

> 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".

So entfernen Sie ein Tag von einem Gerät:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (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-Zuweisen aufheben**.
6. Klicken Sie im folgenden Fenster auf **Ja**.

Das Tag wurde vom Gerät entfernt.

So entfernen Sie Tags von mehreren Geräten:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
2. Wählen Sie die Geräte aus, deren Tags Sie entfernen möchten.
3. Klicken Sie auf **Tags** und wählen Sie anschließend in der Dropdown-Liste die Option **Zuweisen aufheben** aus.

4. Aktivieren Sie im neuen Fenster die Kontrollkästchen neben den Tags, die Sie entfernen möchten.

   Im Fenster werden alle Tags angezeigt, die allen Geräten zugewiesen sind, die Sie in Schritt 2 ausgewählt haben.

5. Klicken Sie auf **Speichern**.

Die Tags wurden von den Geräten entfernt.

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 **Asset-Verwaltung** → **Tags** → **Regeln für die automatische Tag-Zuweisung**.
- Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **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 Next Expert View verwenden, die Unterscheidung zwischen Groß- und Kleinschreibung aktiviert 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.

   - **Anwendungen** – Vorhandensein eines Administrationsagenten auf dem Gerät, Typ des Betriebssystems, Version, Architektur und Paketmanager.
   - **Virtuelle Maschinen** – Das Gerät gehört zu einem speziellen Typ für virtuelle Maschinen.
   - **Active Directory** – 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. Starten Sie die Eingabeaufforderung mit Root-Berechtigungen 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. Das Standardverzeichnis für die Installation ist /opt/kaspersky/klnagent64/sbin/.

2. Geben Sie einen der folgenden Befehle ein:

   - So weisen Sie einen Satz mit Tags zu:

     ```
     /opt/kaspersky/klnagent64/sbin/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:

     ```
     /opt/kaspersky/klnagent64/sbin/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:

     ```
     /opt/kaspersky/klnagent64/sbin/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:

     ```
     /opt/kaspersky/klnagent64/sbin/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.

Quarantäne und Datei-Backups

Auf den Client-Geräten installierte Antiviren-Programme von Kaspersky können während der Untersuchung der Geräte die Dateien in die Quarantäne oder in das Datei-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.

Die *Datei-Backups* dienen zur Speicherung der Backup-Kopien von Dateien, die gelöscht oder bei der Desinfizierung verändert wurden.

Kaspersky Next Expert View erstellt eine zusammengefasste Liste von Dateien, die von Kaspersky-Anwendungen auf den Client-Geräten in die Quarantäne oder in Datei-Backups verschoben werden. Die Administrationsagenten der Client-Geräte leiten Informationen über die Dateien in der Quarantäne und in den Datei-Backups an den Administrationsserver weiter.

Kaspersky Next Expert View kopiert keine Dateien aus der Datenverwaltung auf den Administrationsserver. Alle Dateien werden in der Datenverwaltung auf den Geräten abgelegt.

Eine Datei aus der Datenverwaltung herunterladen

Kaspersky Next Expert View ermöglicht es, Kopien von Dateien herunterzuladen, die von einer Sicherheitsanwendung in die Quarantäne oder in das Datei-Backups des Client-Geräts verschoben wurden. Die Dateien werden in das von Ihnen angegebene Ziel kopiert.

Sie können Dateien nur herunterladen, wenn eine folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird ein Push-Server verwendet oder es wird ein Verbindungsgateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

So speichern Sie die Kopie einer Datei aus der Quarantäne oder dem Datei-Backups 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 Datei-Backups speichern möchten, wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Datei-Backups**.

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.

Dateien aus der Datenverwaltung entfernen

So löschen Sie eine Datei aus der Quarantäne oder dem Datei-Backups:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** und wählen Sie anschließend einen der folgenden Abschnitte aus:

   - **Quarantäne**, wenn Sie eine Datei aus der Quarantäne löschen möchten.

   - **Datei-Backups**, wenn Sie eine Datei aus dem Backup löschen möchten.

2. Führen Sie entsprechend der von Ihnen ausgewählten Datenverwaltung einen der folgenden Schritte aus:

   - Wählen Sie für den Abschnitt **Datei-Backups** die Datei in der Liste und klicken Sie anschließend auf die Schaltfläche **Entfernen**.

   - Im Abschnitt **Quarantäne** können Sie eine Datei auf folgende Arten löschen:

     - Aktivieren Sie das Kontrollkästchen neben dem Namen der zu löschenden Datei und klicken Sie anschließend in der Symbolleiste auf die Schaltfläche **Löschen**.

     - Klicken Sie zunächst auf den Namen der zu löschenden Datei und anschließend im angezeigten Detailfenster in der Symbolleiste auf die Schaltfläche **Löschen**.

       In diesem Fall wird die Datei gelöscht, eine entsprechende Benachrichtigung auf dem Bildschirm angezeigt und das Detailfenster geschlossen.

Die Sicherheitsanwendung auf dem Client-Gerät mit platzierten Dateien in der Datenverwaltung (Quarantäne oder Datei-Backups) löscht dieselben Dateien aus der Datenverwaltung.

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, gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (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 auf der Registerkarte **Erweitert** 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 **Kaspersky-Anwendungen** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.

3. Wählen Sie in der Programmliste 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 Kaspersky Security-Agenten 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 **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 **Kaspersky-Anwendungen** 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 **Stufe der Xperf-Ablaufverfolgung 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:

   - **Basic**

     Die Ablaufverfolgungsinformationen werden während der Ausführung der Sicherheitsanwendung Kaspersky Endpoint Security empfangen.

     Diese Variante ist standardmäßig ausgewählt.

   - **Bei Neustart**

     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

Sie können Protokolldatei von einem Client-Gerät nur dann herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird ein Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

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 **Kaspersky-Anwendungen** 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.

   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

Sie können die Programmeinstellungen von einem Client-Gerät nur dann herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird ein Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

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 **Kaspersky-Anwendungen** aus.
3. Klicken Sie im Abschnitt **Anwendungseinstellungen** 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.

Systeminformationen von einem Client-Gerät herunterladen

Sie können die Systeminformationen von einem Client-Gerät nur dann auf Ihr eigenes Gerät herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird ein Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

So laden Sie Systeminformationen von einem Client-Gerät herunter:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Systeminformationen** aus.
3. Klicken Sie auf die Schaltfläche **Herunterladen**, um die Systeminformationen über das Client-Gerät herunterzuladen.

Die Datei mit den Informationen wird an den angegebenen Speicherort heruntergeladen.

Ereignisprotokolle downloaden

Sie können die Ereignisprotokolle von Client-Gerät nur dann herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

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.

     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 **Kaspersky-Anwendungen** 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:

   - **Anwendung beenden**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Anwendung neu starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Anwendung 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.

Ausführen der Ferndiagnose eines Programms und Herunterladen der Ergebnisse

Um die Diagnose für ein Programm auf einem Remote-Gerät zu starten und die Ergebnisse 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 **Kaspersky-Anwendungen** 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 Ferndiagnose ausführen möchten.

   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 Supportspezialist von Kaspersky Sie dazu auffordert. Sie müssen das Programm nicht auf dem Gerät installieren.

Wenn Sie auf dem Client-Gerät ein benutzerdefiniertes Skript ausführen möchten, können Sie die Umgebungsvariable `KLACDT_SAVE_SETTING` verwenden, um den Pfad zum Speichern der Ausführungsergebnisse zu bestimmen. Beispielsweise:

- Für ein Gerät auf Windows-Basis:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Für ein Gerät auf Linux-Basis:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

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. Wählen Sie im Feld **Objekttyp** den Objekt-Typ des Objekts, das Sie hochladen möchten:
   - Wählen Sie **Datei**, um die ausführbare Datei hochzuladen.
   - Wählen Sie **Ordner**, um den Ordner mit der Anwendung hochzuladen, die Sie auf dem Client-Gerät ausführen möchten.

     Wenn Sie diesen Objekt-Typ auswählen, wird das Feld **Name der zu startenden ausführbaren Datei** angezeigt. Geben Sie in diesem Feld den Namen der ausführbaren Datei im Ordner an. Sie können auch den relativen Pfad zu der Datei angeben.
   - Wählen Sie **Archiv**, um das zip-Archiv mit der Anwendung hochzuladen, die Sie auf dem Client-Gerät ausführen möchten.

     Wenn Sie diesen Objekt-Typ auswählen, wird das Feld **Name der zu startenden ausführbaren Datei** angezeigt. Geben Sie in diesem Feld den Namen der ausführbaren Datei im Ordner an, die Sie auf dem Client-Gerät ausführen möchten. Sie können auch den relativen Pfad zu der Datei angeben.

     > 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.
4. Laden Sie das Objekt hoch, indem Sie es im Standard-Dialog des Betriebssystems auswählen oder in das Upload-Feld ziehen.
5. Geben Sie bei Bedarf im Feld **Kommandozeilenargumente** die Befehlszeilenargumente an, die beim Ausführen der ausführbaren Datei übergeben werden sollen.
6. Klicken Sie auf die Schaltfläche **Hochladen und ausführen**, um die angegebene Anwendung auf einem Client-Gerät auszuführen.

7. Nachdem die Anwendung erfolgreich ausgeführt wurde, laden Sie die Ausführungsergebnisse herunter, indem Sie auf die Schaltfläche **Ausführungsergebnisse der Anwendung herunterladen** klicken.

   Die Ergebnisse einer Anwendungsausführung werden so lange gespeichert, bis Sie eine erneute Diagnose ausführen oder das Fenster schließen.

Die Ferndiagnose eines Client-Geräts mithilfe der Anwendung ist abgeschlossen.

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 Generieren von Dump-Dateien ist nur für 32-Bit-Prozesse verfügbar, die auf Windows-basierten Client-Geräten ausgeführt werden. Diese Funktion wird für Linux-Client-Geräte und 64-Bit-Prozesse nicht unterstützt.

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 Ferndiagnose-Fenster 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 **Herunterladen**, um die Dump-Datei für die angegebene Anwendung zu speichern.

   Wenn die angegebene Anwendung nicht auf dem Client-Gerät ausgeführt wird, erscheint eine Fehlermeldung.

Remotedesktopverbindung mit dem Client-Gerät herstellen

Sie können 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 bekommen Sie vollständigen Zugriff auf die Informationen dieses Geräts und können 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 Ihrer Workstation befinden. Mit diesem Dienstprogramm können Sie die Verbindung zwischen einem Client-Gerät und dem Administrationsserver tunneln.

  Kaspersky Next Expert View 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 Sie sich mit der Sitzung verbunden haben, wird der Benutzer des Client-Geräts ohne vorherige Benachrichtigung von der Sitzung abgemeldet.

Um sich mittels mit dem Desktop eines Client-Geräts zu verbinden, muss eine der folgenden Voraussetzungen erfüllt sein:

- Das Client-Gerät ist Mitglied einer Administrationsgruppe, die einen Verteilungspunkt mit aktivierter Option **Verbindung mit dem Administrationsserver nicht trennen** besitzt.
- In den Einstellungen des Client-Gerätes ist die Option **Verbindung mit dem Administrationsserver nicht trennen** aktiviert.

  Die Gesamtzahl an Client-Geräten mit aktivierter Option **Verbindung mit dem Administrationsserver nicht trennen** beträgt höchstens 300.

Um eine Verbindung mit Desktop eines Client-Geräts herstellen:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte).**
2. Aktivieren Sie das Kontrollkästchen neben dem Namen des Geräts, für das Sie Zugriff benötigen.

3. Klicken Sie auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster "Mit Remote-Desktop verbinden" wird geöffnet.

4. Klicken Sie auf die Schaltfläche **Herunterladen**, um das Dienstprogramm "klsctunnel" herunterzuladen.

5. 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 "Mit Remote-Desktop verbinden" erneut, um einen neuen BLOB zu generieren.

6. Führen Sie das Dienstprogramm "klsctunnel" aus.

   Das Fenster des Dienstprogramms wird geöffnet.

7. Fügen Sie den kopierten Text in das Textfeld ein.

8. Wenn Sie einen Proxyserver verwenden, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie dann die Verbindungseinstellungen für den Proxyserver ein.

9. Klicken Sie auf die Schaltfläche **Port öffnen**.

   Das Anmeldefenster für die Remotedesktopverbindung wird geöffnet.

10. Geben Sie die Anmeldeinformationen des Kontos an, mit dem Sie derzeit bei Kaspersky Next Expert View angemeldet sind.

11. 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

Sie können 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.

Sie können eine Verbindung mit der vorhandenen Sitzung auf dem Client-Gerät herstellen, ohne dass der Benutzer dieser Sitzung getrennt wird. In diesem Fall haben Sie 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 Ihrer Workstation befinden. Mit diesem Dienstprogramm können Sie die Verbindung zwischen einem Client-Gerät und dem Administrationsserver tunneln.

Kaspersky Next Expert View 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 von Ihnen eine Anfrage zum Herstellen der Verbindung. Es werden keine Informationen über die Aktivitäten auf dem Remote-Gerät und deren Ergebnisse in den Berichten von Kaspersky Next Expert View gespeichert.

  Sie können ein Audit der Benutzeraktionen 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:

- Microsoft Windows Vista oder höher ist auf Ihrer Workstation installiert.

  Um zu prüfen, ob die Funktion für die Windows Desktopfreigabe in Ihrer Windows-Edition enthalten ist, stellen Sie sicher, dass CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} in der 32-Bit-Registry enthalten ist.

- Microsoft Windows Vista oder höher ist auf dem Client-Gerät installiert.
- Kaspersky Next Expert View nutzt eine Lizenz für Schwachstellen- und Patch-Management.
- Das Client-Gerät ist Mitglied einer Administrationsgruppe, die einen Verteilungspunkt mit aktivierter Option **Verbindung mit dem Administrationsserver nicht trennen** besitzt, oder diese Option ist in den Einstellungen des Client-Geräts aktiviert.

  Beachten Sie, dass die maximale Gesamtzahl an Client-Geräten mit aktivierter Option **Verbindung mit dem Administrationsserver nicht trennen** 300 beträgt.

Um eine Verbindung mit dem Client-Gerät-Desktop über Windows Desktopfreigabe herzustellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.
2. Aktivieren Sie das Kontrollkästchen neben dem Namen des Geräts, für das Sie Zugriff benötigen.
3. Klicken Sie auf die Schaltfläche **Windows Desktopfreigabe**.

   Der Assistent für die Windows Desktopfreigabe öffnet sich.
4. 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.
5. Klicken Sie auf die Schaltfläche **Weiter**.

6. Wählen Sie die Sitzung auf dem Gerät, mit dem Sie sich verbinden möchten, und klicken Sie auf **Weiter**.

7. 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.

8. 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.

9. Führen Sie das Dienstprogramm "klsctunnel" aus.

   Das Fenster des Dienstprogramms wird geöffnet.

10. Fügen Sie den kopierten Text in das Textfeld ein.

11. Wenn Sie einen Proxyserver verwenden, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie dann die Verbindungseinstellungen für den Proxyserver ein.

12. 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.

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 Administrationsserver von Kaspersky Next Expert View. 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 Ereignisprotokolle 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 Status finden Sie in der Hilfe zu Kaspersky Endpoint Security.

Anzeigen der Liste der Funde mithilfe der Regeln für die Adaptive Kontrolle von Anomalien

So zeigen Sie die Liste der Funde mithilfe der Regeln für die Adaptive Kontrolle von Anomalien an:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung**.
2. Klicken Sie auf den Link **Auslöser der Regel im Smart-Training-Status**.

   Die Liste enthält die folgenden Informationen zu den Funden mithilfe der Regeln für die Adaptive Kontrolle von Anomalien:

   - **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.

   - **Benutzername**

     Name des Benutzers des Client-Geräts, der den Prozess ausgeführt hat, welcher den Fund erzeugt hat.

   - **Bearbeitet**

     Datum, an dem die Anomalie gefunden wurde.

   - **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).

Um Eigenschaften der einzelnen Informationselemente anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung**.
2. Klicken Sie auf den Link **Auslöser der Regel im Smart-Training-Status**.
3. Wählen Sie im sich öffnenden Fenster das gewünschte Objekt aus.
4. Klicken Sie auf den Link **Eigenschaften**.

   Daraufhin wird das Eigenschaftenfenster des Objekts geöffnet und zeigt Informationen über das ausgewählte Element an.

Sie können jedes Element in der Liste mit Funden der Regeln zur Adaptiven Kontrolle von Anomalien bestätigen oder zu den Ausschlüssen 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 der Elemente wird in **Bestätigung** geändert.

Ihre Bestätigung trägt zu den Statistiken bei, die von den Regeln verwendet werden (weitere Informationen finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows).

Um ein Element als Ausschluss hinzuzufügen, gehen Sie wie folgt vor:

Klicken Sie auf ein Element (oder mehrere Elemente) in der Liste der Funde und anschließend auf die Schaltfläche **Ausschließen**.

Daraufhin wird der Assistent für das Hinzufügen eines Ausschlusses gestartet. Folgen Sie den Schritten des Assistenten.

Wenn Sie ein Element ablehnen oder bestätigen, wird es nach der nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver von der Liste der Funde von adaptiven Anomalien ausgeschlossen und nicht länger in der Liste angezeigt.

Ausschlüsse aus den Regeln zur Adaptiven Kontrolle von Anomalien hinzufügen

Der Assistent für das Hinzufügen eines Ausschlusses erlaubt das Hinzufügen von Ausnahmen aus den Regeln zur Adaptiven Kontrolle von Anomalien für Kaspersky Endpoint Security für Windows.

Um den Assistent für das Hinzufügen eines Ausschlusses über den Knoten "Adaptive Kontrolle von Anomalien" zu starten, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Auslöser der Regel im Smart-Training-Status**.

2. Wählen Sie in dem sich öffnenden Fenster ein Element (oder mehrere Elemente) in der Liste der Funde und klicken Sie anschließend auf die Schaltfläche **Ausschließen**.

   Sie können bis zu 1000 Ausschlüsse auf einmal hinzufügen. Wenn Sie mehr Elemente auswählen und versuchen, diese den Ausnahmen hinzuzufügen, erscheint eine Fehlermeldung.

Der Assistent zum Hinzufügen von Ausnahmen wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

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 wollen.

Administrationsgruppen anlegen

Zu Beginn enthält die Hierarchie der Administrationsgruppen nur eine Administrationsgruppe mit dem Namen **Verwaltete Geräte**. Sie können der Gruppe **Verwaltete Geräte** weitere Geräte und untergeordnete Gruppen hinzufügen.

Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Wählen Sie in der Hierarchie die Administrationsgruppe aus, welche die neue Administrationsgruppe enthalten soll.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.
4. Geben Sie im folgenden Fenster den Namen der Gruppe ein, und klicken Sie auf **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 **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Klicken Sie auf die Schaltfläche **Importieren**.

   Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Schritten 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. Rufen Sie im Hauptmenü den Abschnitt **Asset-Verwaltung** → **Gruppenhierarchie** auf und klicken Sie auf den Namen der gewünschten Administrationsgruppe.

2. Wechseln Sie im neuen Fenster auf die Registerkarte **Automatische Installation**.

3. Wählen Sie die Installationspakete für die Anwendungen aus, die auf den Geräten installiert werden sollen, und bestätigen Sie anschließend auf die Schaltfläche **Speichern**.

   Wenn Sie für eine Anwendung mehrere Installationspakete auswählen, die sich lediglich in ihren Versionen unterscheiden, wird das Installationspaket der aktuellsten Version gespeichert.

Nachdem Sie die Installationspakete ausgewählt haben, wird für jede Anwendung eine Gruppenaufgabe zur Installation der Anwendungen auf den Geräten der Administrationsgruppe erstellt. Diese Aufgaben werden auf den Client-Geräten gestartet, direkt nachdem diese zu der Administrationsgruppe hinzugefügt wurden.

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. Die Anwendung 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 in dem Ordner, in den Sie die Administrationsgruppe verschieben, bereits eine Gruppe mit dem gleichen Namen vorhanden ist, ändern Sie den Namen der zu verschiebenden Administrationsgruppe. 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.

Die Gruppe **Verwaltete Geräte** kann weder umbenannt noch verschoben werden.

So verschieben Sie eine Administrationsgruppe innerhalb der Hierarchie der Administrationsgruppen in eine andere Ebene:

1. Rufen Sie im Hauptmenü den Abschnitt **Asset-Verwaltung** → **Gruppenhierarchie** auf und aktivieren Sie anschließend das Kontrollkästchen neben der Administrationsgruppe, die Sie verschieben möchten.

2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Verschieben**.

3. Wählen Sie im neuen Fenster aus, wohin Sie die Administrationsgruppe verschieben möchten, und klicken Sie anschließend auf die Schaltfläche **Verschieben**.

Das Fenster schließt sich und die Administrationsgruppe wird in eine andere Ebene der Gruppenhierarchie verschoben.

Deleting administration groups

Wenn Sie eine Administrationsgruppe löschen, die sekundäre Administrationsserver, verschachtelte Gruppen, Client-Geräte, Gruppenaufgaben oder für diese Gruppe erstellte Richtlinien enthält, werden diese ebenfalls alle gelöscht.

Bevor eine Administrationsgruppe gelöscht wird, ist es erforderlich, sekundäre Administrationsserver, Gruppen und Client-Geräte daraus zu löschen.

So löschen Sie eine Administrationsgruppe:

1. Rufen Sie im Hauptmenü den Abschnitt **Asset-Verwaltung** → **Gruppenhierarchie** auf und aktivieren Sie anschließend das Kontrollkästchen neben der Administrationsgruppe, die Sie löschen wollen.

2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Löschen**.

   Die Administrationsgruppe wird gelöscht.

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 Next Expert View bietet eine 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.

Sie können keine Administrationsserver-Richtlinie erstellen.

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:

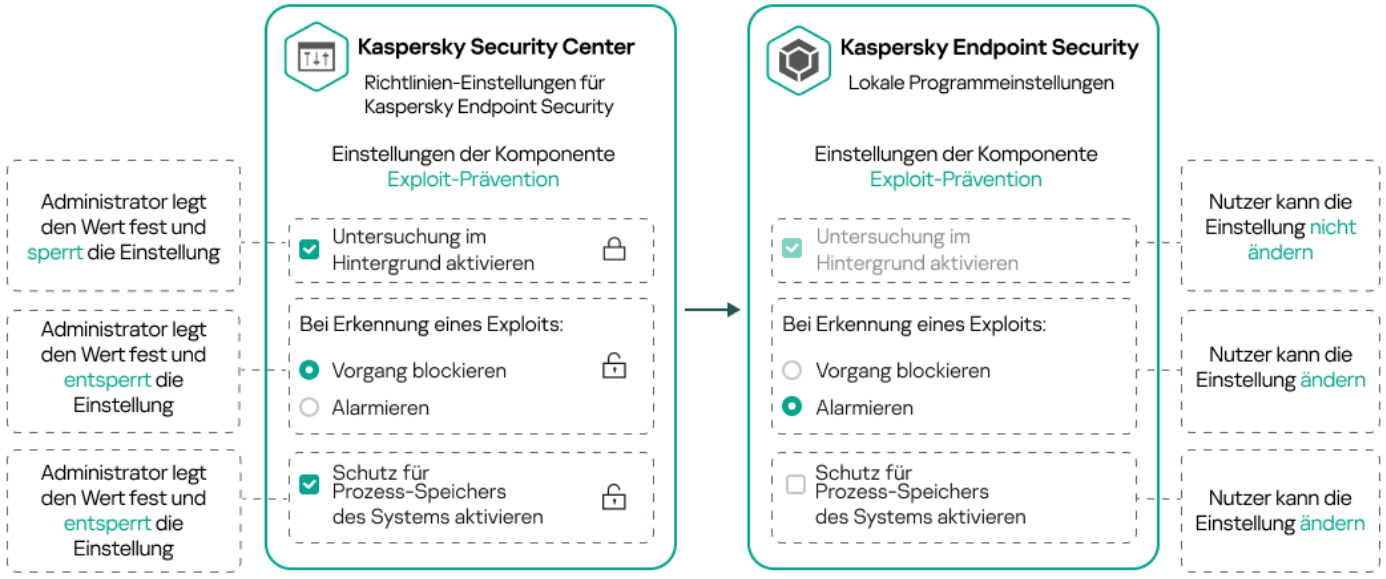
- Sperren von Einstellungen für eine Verwaltungsuntergruppenrichtlinie
- Sperren von Einstellungen einer Kaspersky-Anwendung auf einem verwalteten Gerät

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

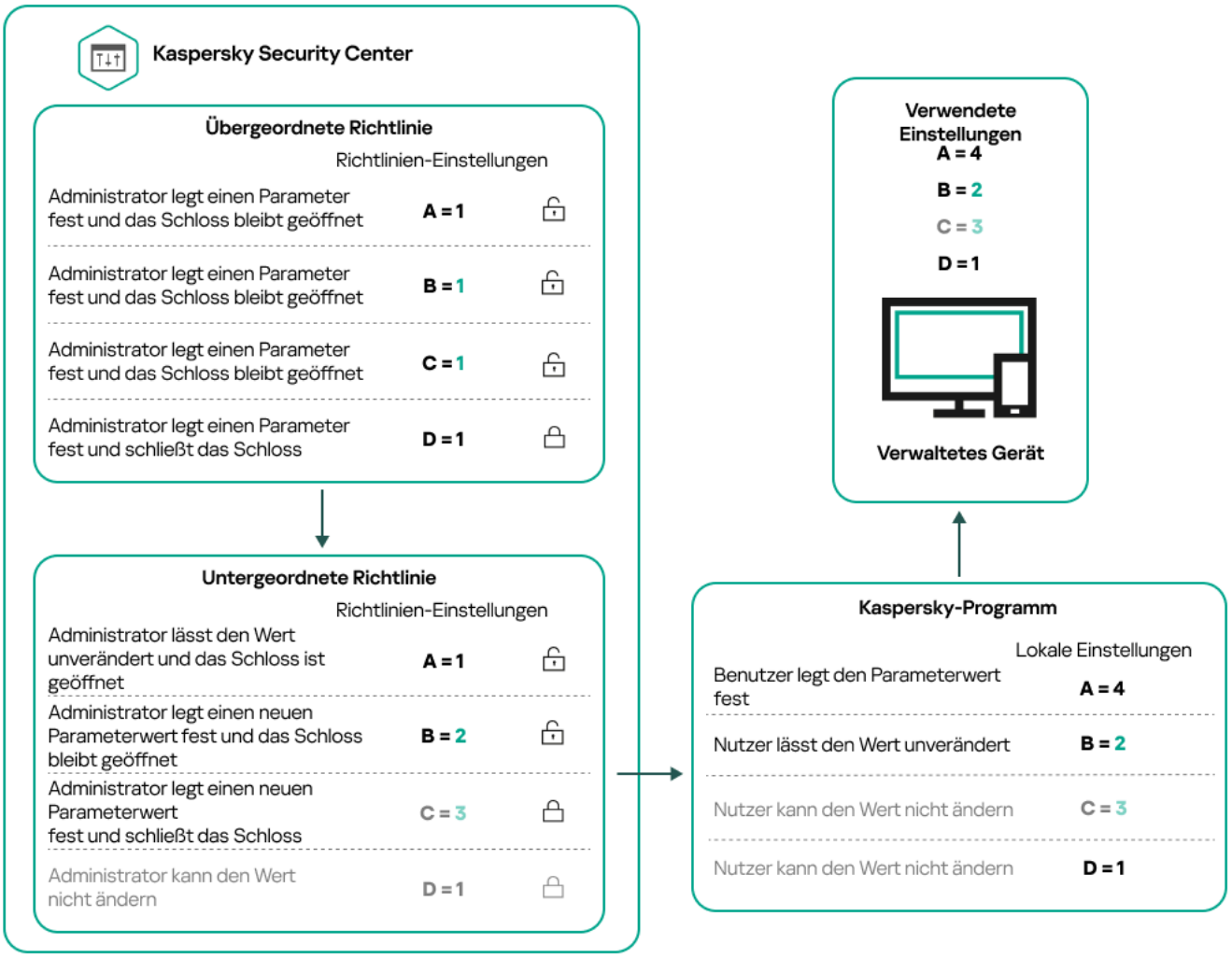
Wenn unterschiedliche Geräte unterschiedliche Einstellungen benötigen, können Sie Geräte in Administrationsgruppen organisieren.

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).

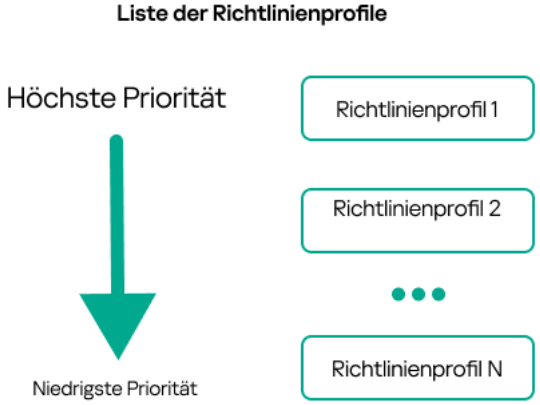


Hierarchie der Richtlinien

Richtlinienprofile in einer Hierarchie von Richtlinien

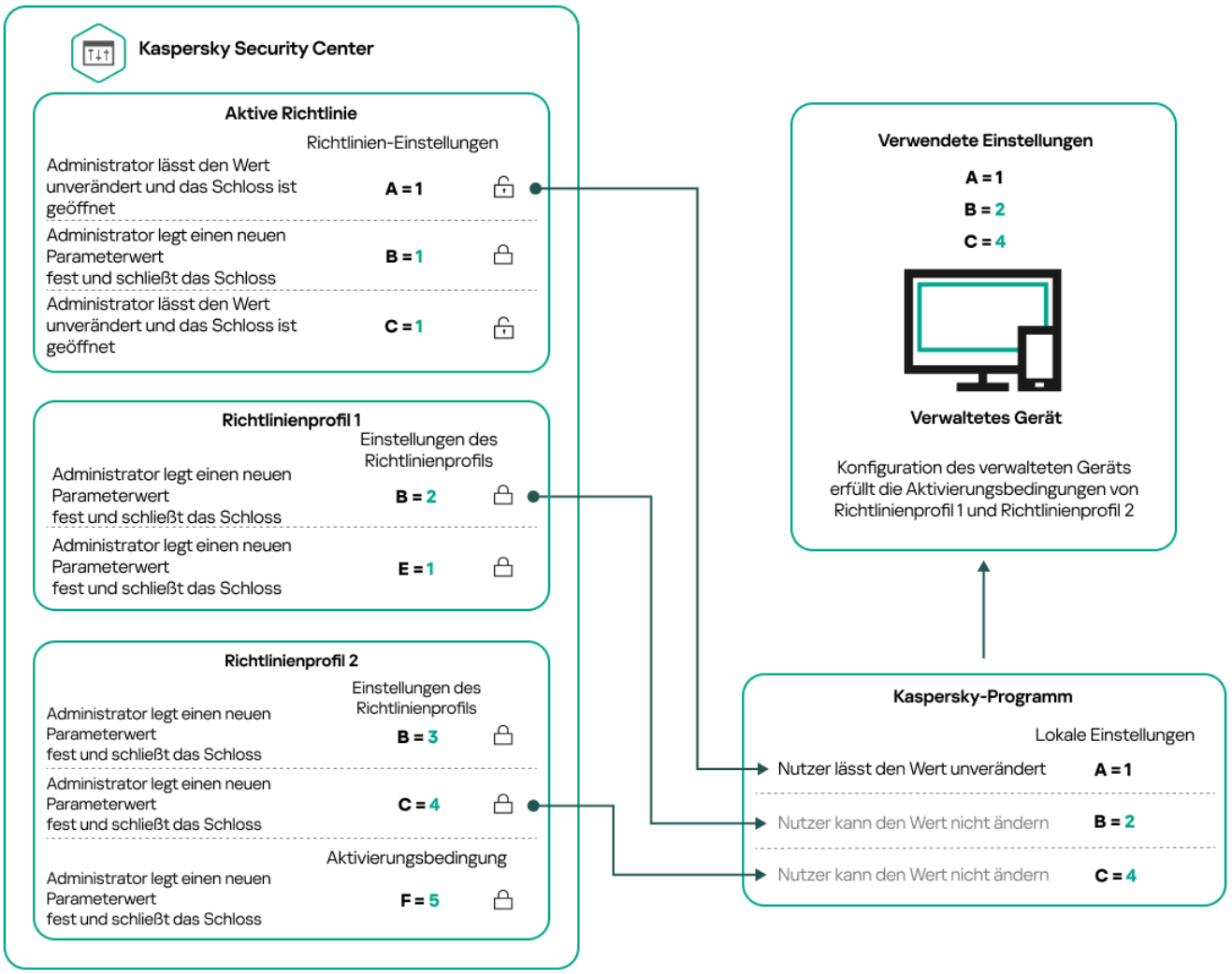
Richtlinienprofile haben die folgenden Bedingungen für die Prioritätszuweisung:

- 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).



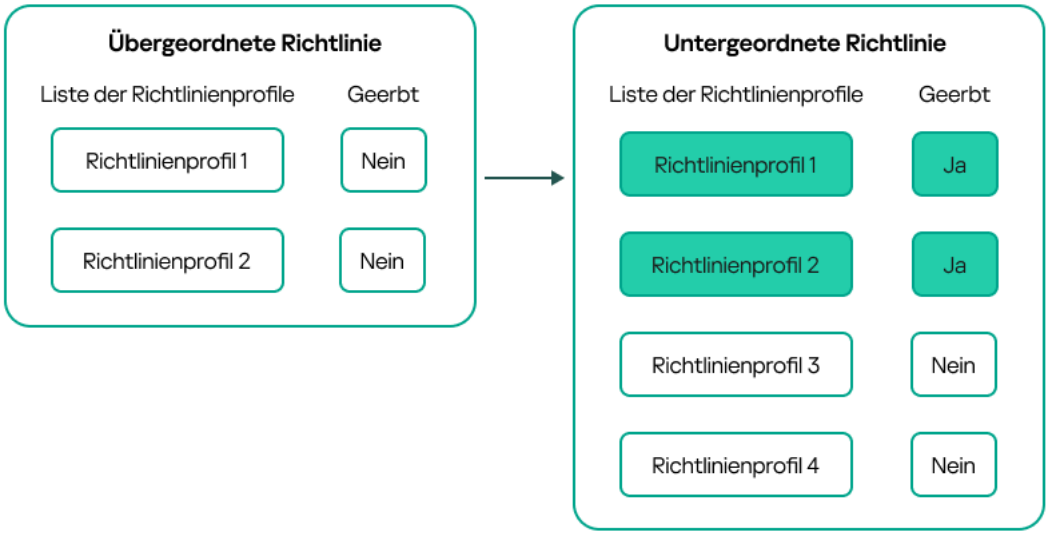
Die Konfiguration des verwalteten Geräts erfüllt die Aktivierungsbedingungen mehrerer Richtlinienprofile.

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 **Asset-Verwaltung** → **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.

> Sie können keine Administrationsserver-Richtlinie erstellen.

Um eine Richtlinie zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
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 der Seite auf die Schaltfläche **Hierarchie anzeigen**.
     Der Name der Schaltfläche ändert sich zu **Hierarchie verbergen**.
     b. Klicken Sie im neuen Fenster auf den Namen der erforderlichen Untergruppe.

Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv. Außerdem können Sie das Hierarchiefenster schließen, indem Sie auf die Schaltfläche **Hierarchie verbergen** klicken.

3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Anwendung 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. Klicken Sie auf die Registerkarte **Anwendungseinstellungen**.

   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 **Anwendungseinstellungen** 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.

   Die Programmeinstellungen sind davon abhängig, für welches Programm 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 **Asset-Verwaltung** → **Richtlinien**.

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**.

   Es wird eine Benachrichtigung mit folgendem Inhalt angezeigt: **Die Richtlinie wird gespeichert und über die Hierarchie der Administrationsserver verteilt**.

   Wenn die Richtlinie die Validierung besteht, wird eine weitere Benachrichtigung angezeigt: **Richtlinie wurde gespeichert**.

   Wenn die Richtlinie die Validierung nicht besteht, wird die folgende Benachrichtigung angezeigt: **Das Speichern und Verteilen der Richtlinie über die Hierarchie der Administrationsserver ist fehlgeschlagen. Wenden Sie sich an den Technischen Support**. Sie können die Richtlinieneinstellungen überprüfen und anpassen und es anschließend erneut versuchen. Wenn das Problem weiterhin besteht, wenden Sie sich an den Technischen Support.

Die Änderungen der Richtlinie werden in den Eigenschaften der Richtlinie gespeichert und im Abschnitt **Revisionsverlauf** angezeigt.

Bei Bedarf können Sie Richtlinienrevisionen vergleichen. Diese Option ist für die Richtlinien der folgenden Komponenten verfügbar: Administrationsserver, Administrationsagent, Kaspersky Endpoint Security für Windows (beginnend ab Version 14.0 des Web-Plug-ins) und Kaspersky Endpoint Security for Mac (beginnend ab Version 12.2.1 Patch A des Web-Plug-ins).

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**
  - **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 **Vererbung von Einstellungen** 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:

  - **In der Administrationsserver-Datenbank speichern für (Tage)**

  - **Im System-Ereignisprotokoll des Geräts speichern**

- **Ereignisbenachrichtigungen**

  Sie können bestimmen, ob Sie per E-Mail über das Ereignis benachrichtigt werden möchten:

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 der Registerkarte **E-Mail** ändern.

Die Registerkarte **Konfiguration von Ereignissen** zeigt Benachrichtigungen an, wenn neue Ereignistypen hinzugefügt wurden (z. B. in einer neuen Version der Anwendung) und erlaubt Ihnen das Anwenden der neuen Einstellungen durch das Anklicken der Schaltfläche **Speichern** oder **Speichern und schließen**.

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie eine Liste mit Revisionen der Richtlinie anzeigen, Richtlinienrevisionen vergleichen 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 **Asset-Verwaltung** → **Richtlinien**.
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 **Asset-Verwaltung** → **Richtlinien**.
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 Next Expert View können Sie eine Richtlinie mit ihren Einstellungen und die 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 **Asset-Verwaltung** → **Richtlinien**.
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 Next Expert View 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 **Asset-Verwaltung** → **Richtlinien**.
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 Next Expert View 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 **Asset-Verwaltung** → **Richtlinien**.

2. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, für die Sie den Verteilungsstatus auf dem Gerät anzeigen wollen.

3. Klicken Sie im sich öffnenden Menü auf den Link **Verteilung**.

   Das Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird geöffnet.

4. Im geöffneten Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird die **Statusbeschreibung (falls verfügbar)** 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. Gehen Sie im Hauptmenü zu **Einstellungen** → **Einstellungen der Benutzeroberfläche**.

2. Geben Sie im Feld **Maximale Anzahl von Geräten, die in den Ergebnissen der Richtlinienverteilung angezeigt werden** die Anzahl der Geräte an (bis zu 100.000).

   Die standardmäßige Anzahl beträgt 5000.

3. Klicken Sie auf die Schaltfläche **Speichern**.

Ihre Einstellungen werden gespeichert und übernommen.

Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren

Damit beim Ereignis "Virenangriff" automatisch eine Richtlinie aktiviert wird:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster für die Einstellungen des Administrationsservers wird mit der Registerkarte **Allgemein** geöffnet.

2. Wählen Sie den Abschnitt **Virenangriff** aus.

3. Klicken Sie im rechten Bereich auf den Link **Richtlinien so konfigurieren, dass sie aktiviert werden, wenn ein Ereignis des Typs "Virenangriff" auftritt**.

   Das Fenster **Aktivierung von Richtlinien** wird geöffnet.

4. Wählen Sie im Abschnitt der Komponente, die den Virenangriff erkannt hat (Anti-Virus für Workstations und Dateiserver, Anti-Virus für E-Mail-Server oder Anti-Virus für Perimeterschutz) die Optionsschaltfläche neben dem gewünschten Eintrag und klicken Sie auf **Hinzufügen**.

   Ein Fenster mit der Administrationsgruppe **Verwaltete Geräte** wird geöffnet.

5. Klicken Sie auf den Chevron-Symbol (›) neben **Verwaltete Geräte**.

   Eine Hierarchie der Administrationsgruppen und der entsprechenden Richtlinien wird angezeigt.

6. Klicken Sie in der Hierarchie der Administrationsgruppen und Richtlinien auf den Namen einer oder mehrere Richtlinien, die aktiviert werden sollen, wenn ein Virenangriff erkannt wird.

   Um alle Richtlinien in der Liste oder in einer Gruppe auszuwählen, aktivieren Sie das Kontrollkästchen neben dem entsprechenden Namen.

7. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Fenster mit der Hierarchie der Administrationsgruppen und Richtlinien wird geschlossen.

Die ausgewählten Richtlinien werden in die Liste der Richtlinien aufgenommen, die aktiviert werden, wenn ein Virenangriff erkannt wird. Bei einem Virenangriff werden die ausgewählten Richtlinien unabhängig davon aktiviert, ob sie aktiv oder inaktiv sind.

Wird eine Richtlinie aufgrund des Ereignisses "Virenangriff" aktiviert, ist eine Rückkehr zur vorherigen Richtlinie nur manuell möglich.

Erzwungene Synchronisierung

Obwohl Kaspersky Next Expert View den Status, die Einstellungen, die Aufgaben und die Richtlinien für die verwalteten Geräte automatisch synchronisiert, kann es in bestimmten Situationen vorkommen, dass Sie genau wissen, ob die Synchronisierung für ein bestimmtes Gerät bereits ausgeführt wurde.

Damit diese Funktion ordnungsgemäß ausgeführt wird, muss die Option **Verbindung mit Administrationsserver nicht trennen** aktiviert sein, und/oder der Verteilungspunkt muss als Push-Server verwendet werden.

Synchronisation eines einzelnen Geräts

So erzwingen Sie die Synchronisierung zwischen dem Administrationsserver und dem verwalteten Gerät:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (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:
   - Führen Sie eine Geräteauswahl durch, um die Geräteliste anzuzeigen.
   - Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)** und wählen Sie anschließend die Administrationsgruppe aus, welche die zu synchronisierenden Geräte enthält.
     - Für die Stammgruppe können Sie mit dem nächsten Schritt fortfahren.
     - Klicken Sie für eine Untergruppe im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen** und anschließend im neuen Fenster auf den Namen der Untergruppe.

       Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv. Außerdem können Sie das Hierarchiefenster schließen, indem Sie auf die Schaltfläche **Hierarchie verbergen** klicken.
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 können Sie 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 **Asset-Verwaltung** → **Assets (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 Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung 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.

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 **Asset-Verwaltung** → **Richtlinien**.
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 der Priorität eines Richtlinienprofils, zum Erstellen eines Richtlinienprofils, zum Kopieren eines Richtlinienprofils, zum Erstellen einer Regel zur Aktivierung eines Richtlinienprofils und zum Löschen, Exportieren und Importieren eines Richtlinienprofils.

Profile einer Richtlinie anzeigen

So zeigen Sie Profile einer Richtlinie an:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
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 **Anwendungseinstellungen** 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 **Anwendungseinstellungen** 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.

- **Netzwerkstandort des Geräts**

  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).

      Beachten Sie, dass auf die Benutzerliste ein Filter angewendet wird und die Liste Gerätebesitzer anzeigt, die interne Benutzer darstellen.

      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 Next Expert View 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).

      Beachten Sie, dass auf die Benutzerliste ein Filter angewendet wird und die Liste Gerätebesitzer anzeigt, die interne Benutzer darstellen.

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 Next Expert View 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:

  - **Größe des Arbeitsspeichers (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 zugeordnete Rollen**

  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 verwendete 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.

- **Gilt für Geräte ohne die angegebenen Tags**

  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:

  - **Mitgliedschaft des Gerätebesitzers in 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.

Richtlinienprofil exportieren und importieren

Sie können ein Richtlinienprofil in einer KLPROF-Datei speichern, ohne eine Richtlinie zu exportieren, und die KLPROF-Datei anschließend nutzen, um das gespeicherte Profil in die Richtlinie zu importieren.

Dadurch können Sie die Einstellungen des Richtlinienprofils schnell wiederherstellen, anstatt sie erneut konfigurieren zu müssen.

Ein Richtlinienprofil wird in die Richtlinie derselben Version der Anwendung importiert, aus der Sie das Profil exportiert haben. Für Anwendungen, welche die Abwärtskompatibilität von Richtlinien unterstützen (z. B. Kaspersky Endpoint Security für Windows), können Sie Richtlinienprofile in verschiedene Versionen der Richtlinie importieren.

So exportieren Sie ein Richtlinienprofil:

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 exportieren möchten.

3. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Exportieren**.

4. Geben Sie im neuen Fenster das Verzeichnis an, in dem Sie die Datei mit dem Richtlinienprofil speichern möchten.

   Bei Bedarf können Sie den Dateinamen ändern.

5. Klicken Sie auf **Speichern**.

Wenn der Vorgang erfolgreich abgeschlossen wurde, wird eine entsprechende Meldung auf dem Bildschirm angezeigt. Andernfalls wird eine Fehlermeldung angezeigt.

So importieren Sie ein Richtlinienprofil:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Importieren**.

3. Wählen Sie im neuen Fenster die KLPROF-Datei mit dem erforderlichen Richtlinienprofil und klicken Sie auf die Schaltfläche **Öffnen**.

   Die maximale Größe einer importierten Datei beträgt 4 MB.

Wenn der Vorgang erfolgreich abgeschlossen wurde, wird eine entsprechende Meldung auf dem Bildschirm angezeigt. Andernfalls wird eine Fehlermeldung angezeigt.

Das Richtlinienprofil wird mit dem Namen importiert, den es beim Export hatte, und nicht mit dem Namen der KLPROF-Datei.
Die Datei wird unabhängig von der Priorität, die das Richtlinienprofil vor dem Export hatte, mit dem Status **Deaktiviert** und der niedrigsten Priorität importiert.

Der Import kann nicht durchgeführt werden:

- Wenn die Richtlinie bereits ein Profil mit demselben Namen besitzt.
- Wenn die Anzahl der Profile in der Richtlinie 100 beträgt.

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 BitLocker-Laufwerkverschlüsselung auf Geräten mit einem Windows-Betriebssystem für Server oder Workstations verwalten.

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 Next Expert View 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 Next Expert View 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 der Kaspersky Next Expert View 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**.

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** → **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. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz**.

3. Öffnen Sie den Abschnitt **Verschlüsselte Laufwerke**, um die Berichte über den Verschlüsselungsstatus der Massenspeichergeräte oder über die Zugriffsrechte auf verschlüsselte Laufwerke zu generieren.

4. 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.

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 Benutzerkonten

In Kaspersky Next Expert View 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 Next Expert View. Sie können Konten von internen Benutzern erstellen. Diese Benutzerkonten werden nur in Kaspersky Next Expert View verwendet.

So zeigen Sie Tabellen mit Benutzerkonten und Sicherheitsgruppen an:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
2. Wählen Sie die Registerkarte **Benutzer** oder **Gruppen** aus.

Die Tabelle mit den Benutzern oder Sicherheitsgruppen wird geöffnet. Standardmäßig wird die geöffnete Tabelle nach den Spalten **Typ des Kontos** und **Zugeordnete Rollen** gefiltert. In der Tabelle werden interne Benutzer oder Gruppen angezeigt, denen Rollen zugewiesen wurden.

Wenn Sie in der Tabelle nur die Benutzerkonten von lokalen Benutzern anzeigen möchten, setzen Sie das Filterkriterium **Typ des Kontos** auf **Lokal**.

Wenn Sie auf einen sekundären Administrationsserver wechseln, der älter als einschließlich Version 14.2 ist, und anschließend die Liste der Benutzer oder Sicherheitsgruppen öffnen, wird die geöffnete Tabelle nur nach der Spalte **Typ des Kontos** gefiltert. Der Filter nach der Spalte **Zugeordnete Rollen** wird standardmäßig nicht angewendet. Die gefilterte Tabelle enthält alle internen Benutzer oder Sicherheitsgruppen mit und ohne der zugewiesenen Rolle.

Hinzufügen eines Benutzerkontos eines internen Benutzers

In Kaspersky Next Expert View können Sie dem Arbeitsbereich neue Benutzer hinzufügen. Beispielsweise können Sie den hinzugefügten Benutzer als Gerätebesitzer zuweisen.

Hinzufügen eines Benutzerkontos eines internen Benutzers:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
2. Klicken Sie auf der Registerkarte „**Benutzer**“ auf „**Hinzufügen**“.
3. Geben Sie im neuen Fenster **Benutzer hinzufügen** die E-Mail-Adresse des Benutzers ein, den Sie hinzufügen möchten, und klicken Sie anschließend auf **Weiter**.
4. Überprüfen und bearbeiten Sie die Benutzerdaten.
5. Klicken Sie auf „**Fertigstellen**“, um die Änderungen zu übernehmen.

Das Benutzerkonto eines internen Benutzers wird hinzugefügt und in der Benutzerliste angezeigt.

So ändern Sie das Kennwort eines internen Benutzerkontos:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
2. Klicken Sie auf den Namen des Benutzerkontos, das Sie bearbeiten möchten.
3. Ändern Sie auf dieser Seite die Benutzerinformationen:
4. Klicken Sie auf „**Speichern**“, um die Änderungen zu übernehmen.

Damit sich der hinzugefügte interne Benutzer bei der Web Console anmelden und den Arbeitsbereich verwalten kann, können Sie ihm in Kaspersky Next Expert View die Administratorrechte für den Arbeitsbereich erteilen. Sie können das Benutzerkonto eines internen Benutzers auch löschen.

Löschen eines Benutzerkontos eines internen Benutzers

Löschen eines Benutzerkontos eines internen Benutzers:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
2. Aktivieren Sie das Kontrollkästchen neben der Benutzergruppe, die Sie löschen möchten.
3. Klicken Sie auf **Löschen**.
4. Bestätigen Sie das Löschen.

Das Konto eines internen Benutzers wird gelöscht und kann nicht wiederhergestellt werden.

Arbeitsbereichsadministratoren zuweisen

In Kaspersky Next Expert View können Sie Benutzern Administratorrechte für Arbeitsbereiche erteilen. Arbeitsbereichsadministratoren können sich bei der Web Console anmelden und den Arbeitsbereich verwalten.

So weisen Sie einen Arbeitsbereichsadministrator zu:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
2. Klicken Sie auf der Registerkarte „**Benutzer**“ auf den Namen des Benutzers, dem Sie die Rolle eines Arbeitsbereichsadministrators zuweisen möchten.
3. Aktivieren Sie im sich öffnenden Fenster den Schalter „**Arbeitsbereich-Administrator**“.
4. Klicken Sie auf „**Speichern**“, um die Änderungen zu übernehmen.

Um die Rechte des Arbeitsbereich-Administrators zu widerrufen, deaktivieren Sie den Schalter „**Arbeitsbereich-Administrator**“.

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, einschließlich virtueller, weitergeben.

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.

Zugriffsrechte auf Programmfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle

Kaspersky Next Expert View bietet Unterstützungen für eine rollenbasierte Zugriffskontrolle auf die Funktionen von Kaspersky Next Expert View und von verwalteten Kaspersky-Anwendungen an.

Sie können die Zugriffsrechte auf Programmfunktionen für Benutzer von Kaspersky Next Expert View 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 nachfolgende Tabelle gibt die Funktionen von Kaspersky Next Expert View 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 auf Geräteauswahl durchführen** 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: Grundlegende Funktionen**.

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
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	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
Allgemeine Funktionen: **Zugriff auf Objekte, unabhängig von ihren ACLs**	**Lesen**	Lesezugriff auf alle Objekte erhalten: **Lesen**	Nichts	Nichts
Allgemeine Funktionen: **Grundlegende Funktionen**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Regeln für das Verschieben von Geräten (erstellen, ändern, löschen) für den virtuellen Server: **Schreiben**, **Vorgänge auf 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**	• "Download von Updates in die Datenverwaltung des Administrationsservers" • "Berichte senden" • "Installationspaket verteilen" • "Remote-Installation einer Anwendung auf sekundären Administrationsservern"	• "Bericht über de Schutzstatus" • "Bericht über Bedrohungen" • "Bericht über die stärksten infizier Geräte" • "Bericht über de Status der Antiv Datenbanken" • "Fehlerbericht" • "Bericht über Netzwerkangriff • "Zusammenfasse Bericht über inst Schutzprogramr das E-Mail-Syste • "Zusammenfasse Bericht über inst Programme für Perimeterschutz • "Zusammenfasse Bericht über inst Anwendungsart • "Bericht über die Benutzer infizier Geräte" • "Sicherheitsvorf melden" • "Ereignisbericht" • "Bericht über die Aktivität von Verteilungspunk

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
				• "Bericht über sekundäre Administrationss • "Bericht über die Ereignisse der Gerätekontrolle" • "Bericht über Schwachstellen" • "Bericht über verbotene Progr • "Bericht über die Kontrolle" • "Bericht über de Verschlüsselung verwalteter Gerä • "Bericht über de Verschlüsselung der Massenspeicher • "Bericht über Fe der Dateiverschlüsse • "Bericht über blo Zugriffe auf verschlüsselte D • "Bericht über Berechtigungen Zugriff auf verschlüsselte G • "Bericht über ge Benutzerrechte" • "Bericht über Berechtigungen"
Allgemeine Funktionen: **Gelöschte Objekte**	• **Lesen** • **Schreiben**	• Gelöschte Objekte im Papierkorb anzeigen: **Lesen** • Objekte aus dem Papierkorb löschen: **Schreiben**	Nichts	Nichts
Allgemeine Funktionen: **Verarbeitung von Ereignissen**	• **Ereignisse löschen** • **Einstellungen der Ereignisbenachrichtigung bearbeiten** • **Einstellungen der Ereignisprotokollierung bearbeiten** • **Schreiben**	• Einstellungen der Ereignisregistrierung ändern: **Einstellungen der Ereignisprotokollierung bearbeiten** • Einstellungen der Ereignisbenachrichtigung ändern: **Einstellungen der Ereignisbenachrichtigung bearbeiten** • Ereignisse löschen: **Ereignisse löschen**	Nichts	Nichts
Allgemeine Funktionen: **Verteilung von Programmen von Kaspersky**	• **Patches von Kaspersky verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	Die Installation von Patches akzeptieren oder ablehnen: **Patches von Kaspersky verwalten**	Nichts	• "Bericht über die Lizenzschlüsseln des virtuellen Administrationss • "Bericht über Ve der Kaspersky-Programme" • "Bericht über inkompatible Anwendungen"

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
				• "Bericht über Up Versionen der Kaspersky-Prog Module" • "Bericht über die Bereitstellung de Schutzes"
Allgemeine Funktionen: **Verwaltung von Lizenzschlüsseln**	• **Schlüsseldatei exportieren** • **Schreiben**	• Schlüsseldatei exportieren: **Schlüsseldatei exportieren** • Einstellungen des Lizenzschlüssels des Administrationsservers ändern: **Schreiben**	Nichts	Nichts
Allgemeine Funktionen: **Erzwungene Berichtsverwaltung**	• **Lesen** • **Schreiben**	• Berichte unabhängig von ihren ACLs erstellen: **Schreiben** • Berichte unabhängig von ihren ACLs exportieren: **Lesen**	Nichts	Nichts
Allgemeine Funktionen: **Hierarchie von Administrationsservern**	**Hierarchie von Administrationsservern konfigurieren**	Sekundäre Administrationsserver registrieren, aktualisieren oder löschen: **Hierarchie von Administrationsservern konfigurieren**	Nichts	Nichts
Allgemeine Funktionen: **Benutzerrechte**	**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	Nichts
Allgemeine Funktionen: **Virtuelle Administrationsserver**	• **Virtuelle Administrationsserver verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf 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	"Bericht über die Installationsergebnis Updates für Drittanb Programme"

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel	**Schreiben**	Importieren von Chiffrierschlüsseln: **Schreiben**	Nichts	Nichts
Systemverwaltung: **Verbindungen**	• **RDP-Sitzungen starten** • **Zu bestehenden RDP-Sitzungen verbinden** • **Tunnelung initiieren** • **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Desktop-Sharing-Sitzung erstellen: **Das Recht zum Erstellen einer Desktop-Sharing-Sitzung** • RDP-Sitzungen erstellen: **Zu bestehenden RDP-Sitzungen verbinden** • Tunnel erstellen: **Tunnelung initiieren** • Liste mit Content-Netzwerken speichern: **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern**	Nichts	"Bericht über Gerätebenutzer"
Systemverwaltung: **Hardware-Inventarisierung**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Objekt der Hardware-Inventarisierung abrufen oder exportieren: **Read** • Objekt der Hardware-Inventarisierung hinzufügen, einstellen oder löschen: **Schreiben**	Nichts	• "Bericht über da Hardware-Regist • "Bericht über Veränderungen Konfiguration" • "Hardwareberich
Systemverwaltung: **Network Access Control**	• **Lesen** • **Schreiben**	• CISCO-Einstellungen anzeigen: **Lesen** • CISCO-Einstellungen ändern: **Schreiben**	Nichts	Nichts
Systemverwaltung: **Bereitstellung des Betriebssystems**	• **Bereitstellung von PXE-Servern** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf 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 auf Basis eines Referenzimages von einem Betriebssystem erstellen"	Nichts
Systemverwaltung: **Schwachstellen- und Patch-Management**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Eigenschaften von Patches von Drittanbietern anzeigen: **Lesen** • Eigenschaften von Patches von Drittherstellern ändern: **Schreiben**	• "Windows-Updates synchronisieren" • "Updates von Windows Update installieren" • "Schwachstellen schließen" • "Erforderliche Updates installieren und Schwachstellen schließen"	"Bericht über Prograr Updates"
Systemverwaltung: **Remote-Installation**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf 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	Nichts
Systemverwaltung: **Software-Inventur**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	Nichts	Nichts	• "Bericht über installierte Progr • "Bericht über de Verlauf der Prog Registry"

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
				• "Bericht über de Status lizenziert Programmgrupp • "Bericht über Drittanbieter-Lizenzschlüssel"

Vorkonfigurierte Benutzerrollen

Benutzerrollen, die Benutzern von Kaspersky Next Expert View zugewiesen werden, gewähren Zugriffsrechte für Programmfunktionen.

Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Sie können entweder vorkonfigurierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen und die notwendigen Berechtigungen selbst konfigurieren. Einige der in Kaspersky Next Expert View verfügbaren, vorkonfigurierten Rollen können entsprechenden beruflichen Positionen, wie bspw. **Auditor**, **Security Officer** oder **Supervisor** zugeordnet werden (Diese Rollen stehen in Kaspersky Next Expert View 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	Erlaubt alle Vorgänge in den folgenden 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**.

Rolle	Beschreibung
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**.
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**.

Rolle	Beschreibung
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.
Senior Security Analyst	Gewährt die Berechtigungen **Lesen** in dem Funktionsbereich **Allgemeine Funktionen**: **Grundlegende Funktionen**. 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**. Gewährt die Berechtigung zum Zugriff auf die Lösung Kaspersky Endpoint Detection and Response Expert.
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** im Funktionsbereich **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:
   - **Asset-Verwaltung → Gruppenhierarchie**
   - **Asset-Verwaltung → Aufgaben**
   - **Überwachung → Berichte**

- **Asset-Verwaltung → Geräteauswahlen**
- **Überwachung → 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 auf den Namen des Administrationsservers.

   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
  - Anwendungsintegration
  - 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.

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 Schritten 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.

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, Benutzergruppen 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 Benutzergruppen, 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 Benutzergruppen 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 Benutzergruppen aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.

7. Klicken Sie auf die Schaltfläche **Rolle zuordnen**, um das Fenster zu schließen.

8. Schließen Sie das Fenster mit den Rolleneigenschaften.

Die ausgewählten Benutzer oder Benutzergruppen und die ausgewählte Administrationsgruppe werden dem Bereich der Benutzerrolle hinzugefügt.

Methode 3:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   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, klicken Sie dann auf **OK** und speichern Sie die Änderungen.

   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**.
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.

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 **Neue Gruppe**.

3. Geben Sie im Fenster **Neue Gruppe** die folgenden Einstellungen für die neue Sicherheitsgruppe an:

   - **Name**

   - **Beschreibung**

4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Eine neue Sicherheitsgruppe wird zur Liste mit Sicherheitsgruppen hinzugefügt.

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.

Benutzerkonten zu einer internen Gruppe hinzufügen

Einer internen Gruppe können nur Benutzerkonten interner Benutzer hinzugefügt werden.

So fügen Sie einer internen Gruppe Benutzerkonten hinzu:

1. Wechseln 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 eine Gruppe hinzufügen möchten.
3. Klicken Sie auf die Schaltfläche **Gruppe zuordnen**.
4. Wählen Sie im folgenden Fenster **Gruppe zuordnen** die Gruppe aus, der Sie Benutzerkonten hinzufügen möchten.
5. Klicken Sie auf die Schaltfläche **Zuweisen**.

Die Benutzerkonten werden der Gruppe hinzugefügt. Sie können interne Benutzer auch mithilfe der Gruppeneinstellungen zu einer Gruppe hinzufügen.

Löschen einer Sicherheitsgruppe

Sie können nur interne Sicherheitsgruppen löschen.

So löschen Sie eine Benutzergruppe:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Gruppen** aus.
2. Aktivieren Sie das Kontrollkästchen neben der Benutzergruppe, die Sie löschen möchten.
3. Klicken Sie auf **Löschen** und bestätigen Sie im neuen Fenster den Löschvorgang.

Die Benutzergruppe ist gelöscht.

ADFS-Integration konfigurieren

Damit sich die in Active Directory (AD) registrierten Benutzer Ihres Unternehmens an der Kaspersky Next Expert View anmelden können, müssen Sie die Integration mit Active Directory Federation Services (AD FS) konfigurieren.

Kaspersky Next Expert View unterstützt AD FS 3 (Windows Server 2016) oder eine neuere Version. AD FS muss veröffentlicht und über das Internet verfügbar sein. AD FS verwendet ein öffentliches vertrauenswürdiges Zertifikat für die Kommunikation des Dienstes.

Um die Einstellungen der AD FS-Integration zu ändern, benötigen Sie die Zugriffsberechtigung zum Ändern von Benutzerberechtigungen.

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die Abfrage der Active Directory abgeschlossen haben.

So konfigurieren Sie die Integrität von AD FS:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Integrationseinstellungen für AD FS** aus.
3. Kopieren Sie die Callback-URL.

   Sie benötigen diese URL, um die Integration in der AD FS-Verwaltungskonsole zu konfigurieren.
4. Fügen Sie in der AD FS-Verwaltungskonsole eine neue Anwendungsgruppe hinzu und fügen Sie anschließend durch Auswählen der Vorlage für die **Server-Anwendung** eine neue Anwendung hinzu (die Namen der Elemente der Microsoft-Benutzeroberfläche werden auf Englisch/Deutsch angegeben).

   Die AD FS-Verwaltungskonsole generiert eine Client-ID für die neue Anwendung. Sie benötigen die Client-ID, um die Integration in Kaspersky Next Expert View zu konfigurieren.
5. Geben Sie als Redirect-URI die Callback-URL an, die Sie im Eigenschaftenfenster des Administrationsservers kopiert haben.
6. Generieren Sie ein Client-Secret. Sie benötigen das Client-Secret, um die Integration in Kaspersky Next Expert View zu konfigurieren.
7. Speichern Sie die Eigenschaften der hinzugefügten Anwendung.

8. Fügen Sie der erstellten Anwendungsgruppe eine neue Anwendung hinzu. Wählen Sie dieses Mal das Template **Web-API** aus.

9. Fügen Sie auf der Registerkarte **Identifikatoren** die Client-ID der Serveranwendung, die Sie zuvor hinzugefügt haben, zur Liste **Identifikatoren vertrauenswürdiger Teilnehmer** hinzu.

10. Wählen Sie auf der Registerkarte **Client-Berechtigungen**, in der Liste **Zulässige Bereiche** die Bereiche **allatclaims** und **openid** aus.

11. Fügen Sie auf der Registerkarte **Transformationsregeln für die Ausstellung** eine neue Regel hinzu, indem Sie die das Template **LDAP-Attribute als Claims senden** auswählen:

    a. Geben Sie der Regel einen Namen. Sie können sie beispielsweise "Gruppen-SID" nennen.

    b. Wählen Sie **Active Directory** als Attributspeicher aus und ordnen sie anschließend **Token-Gruppen als SIDs** als LDAP-Attribut für 'Gruppen-SID' als ausgehenden Claim-Typ zu.

12. Fügen Sie auf der Registerkarte **Transformationsregeln für die Ausstellung** eine neue Regel hinzu, indem Sie die das Template **Claims mit benutzerdefinierter Regel senden** auswählen:

    a. Geben Sie der Regel einen Namen. Sie können diese beispielsweise "ActiveDirectoryUserSID" nennen.

    b. Geben Sie In dem Feld **Benutzerdefinierte Regel** Folgendes ein:

    ```
    c:[Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
    Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
    ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
    ";objectSID;{0}", param = c.Value);
    ```

13. Öffnen Sie in der Kaspersky Next Expert View den Abschnitt **Integrationseinstellungen für AD FS** erneut.

14. Stellen Sie den Umschalter auf die Position **Integration von AD FS Aktiviert**.

15. Klicken Sie auf den Link **Einstellungen** und geben Sie anschließend die Datei an, die das Zertifikat oder mehrere Zertifikate für den Federation-Server enthält.

16. Klicken Sie auf den Link **Integrationseinstellungen für AD FS** und legen Sie anschließend die folgenden Einstellungen fest:

    - **Aussteller-URL**

      Die URL-Adresse des Federation-Servers, der in Ihrer Organisation läuft.

      In diesem Fall fügt Kaspersky Next Expert View der URL-Adresse des Ausstellers "/.well-known/openid-configuration" hinzu und versucht die resultierende Adresse (issuer_URL/.well-known/openid-configuration) zu öffnen, um die Konfiguration des Ausstellers automatisch zu erkennen.

    - **Client-ID**

      Client-ID, die der Federation-Server generiert, um die Kaspersky Next Expert View zu identifizieren. Die Client-ID finden Sie in der AD FS-Verwaltungskonsole im Eigenschaftenfenster der Serveranwendung, die der Kaspersky Next Expert View entspricht.

    - **Client-Secret**

      Das Client-Secret generieren Sie in der AD FS-Verwaltungskonsole, wenn Sie die Eigenschaften der Serveranwendung angeben, die der Kaspersky Next Expert View entspricht.

- **Domäne, deren Benutzer authentifiziert werden sollen**

  Die Mitglieder der ausgewählten Domäne können sich mit ihren Zugangsdaten für das Domänenkonto an der Kaspersky Next Expert View anmelden. Die Domänennamen werden in der Liste angezeigt, nachdem Sie die Netzwerkabfrage abgeschlossen haben.

- **Feldname der Benutzer-SID im ID-Token**

  Name des Felds, das auf die Benutzer-SID im ID-Token verweist. Der Feldname wird benötigt, um den Benutzer an der Kaspersky Next Expert View zu identifizieren. Standardmäßig heißt dieses Feld im ID-Token "primarysid".

- **Feldname des Arrays mit den Benutzergruppen-SIDs im ID-Token**

  Name des Felds, das sich auf das Array mit den SIDs von Sicherheitsgruppen aus Active Directory bezieht, in denen der Benutzer enthalten ist. Standardmäßig heißt dieses Feld im ID-Token "groupsid".

17. Speichern Sie die Einstellungen.

Die Integration mit AD FS ist abgeschlossen. Um sich mit den Zugangsdaten eines AD-Kontos an der Kaspersky Next Expert View anzumelden, verwenden Sie den Link aus dem Abschnitt **Integrationseinstellungen für AD FS** (**Link zur AD FS-basierten Anmeldung bei Kaspersky Next**).

Nachdem Sie sich mit den Anmeldeinformationen eines AD-Kontos in Kaspersky Next Expert View angemeldet haben, gelten die folgenden Einschränkungen:

- Der Abschnitt „**Data Discovery**“ im Hauptmenü ist nicht verfügbar.
- Der Eintrag **Benutzerkonto verwalten** ist im oberen Bereich nicht verfügbar.
- Sie können nicht zwischen Arbeitsbereichen wechseln.

Wenn Sie sich zum ersten Mal mittels AD FS an der Kaspersky Next Expert View anmelden, reagiert die Konsole möglicherweise mit einer Verzögerung.

Integration mit Microsoft Entra ID konfigurieren

Damit sich die Benutzer in Ihrem Unternehmen mit deren Anmeldedaten von Microsoft Entra ID an der Kaspersky Next Expert View anmelden können, müssen Sie müssen die Integration mit Microsoft Entra ID konfigurieren.

Die Integration mit Microsoft Entra ID ist nur für den primären Administrationsserver verfügbar. Sie können die Integration nicht für sekundäre oder virtuelle Administrationsserver konfigurieren.

Integrationseinstellungen konfigurieren

So konfigurieren Sie die Integration mit Microsoft Entra ID:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Microsoft Entra ID** aus.

3. Aktivieren Sie den Umschalter für die **Integration von Microsoft Entra ID**.

4. Kopieren Sie die Links aus den folgenden Feldern:

   - **Callback-URL**
   - **URL für Front-Channel-Abmeldung**

     Sie benötigen diese URLs, um Kaspersky Next Expert View im Mandanten von Microsoft Entra ID zu registrieren.

   - **Anmelde-URL**

     Sie benötigen diese URL, damit sich die Benutzer nach Abschluss der Integration mit Microsoft Entra ID mit ihren Anmeldedaten für Microsoft Entra ID im Arbeitsbereich von Kaspersky Next Expert View anmelden können.

5. Melden Sie sich am Microsoft Entra Admin Center an, und wählen Sie anschließend den Mandanten für Ihre Organisation aus.

   Für diesen Mandanten müssen Sie über die Rolle "Globaler Administrator" oder "Anwendungsadministrator" verfügen.

6. Wechseln Sie im Hauptmenü zu **Identität** → **Anwendungen** → **App-Registrierungen** und klicken Sie anschließend auf die Schaltfläche **Neue Registrierung**.

7. Führen Sie neuen Fenster die folgenden Schritte aus:

   - Geben Sie einen Namen für Ihre Kaspersky Next Expert View an.
   - Wählen Sie im Abschnitt **Unterstützte Kontotypen** die Option **Konten nur in diesem Organisationsverzeichnis (nur <Mandanten-Name> – Einzelner Mandant) auswählen** aus.
   - Wählen Sie im Abschnitt **Umleitungs-URI** in der Dropdown-Liste **Web** aus und geben Sie die Callback-URL ein, die Sie in Schritt 4 aus Kaspersky Next Expert View kopiert haben.

8. Klicken Sie auf die Schaltfläche **Registrieren**.

   Kaspersky Next Expert View wird in Microsoft Entra ID registriert und die Seite mit der Anwendungsübersicht wird geöffnet.

9. Bei Bedarf können Sie Kaspersky Next Expert View zur Liste der Programme hinzufügen.

   Die Benutzer können anschließend Kaspersky Next Expert View öffnen, ohne die Anmelde-URL verwenden zu müssen. Stattdessen können Sie in der Liste der Programme unter Meine Apps oder im Launcher von Office 365 direkt auf den Namen der Anwendung klicken.

10. Kopieren Sie die **Anwendungs-ID (Client)** und die **Verzeichnis-ID (Mandant)** und speichern Sie sie auf beliebige Weise.

    Sie benötigen diese IDs, wenn Sie die Pflichtfelder in Kaspersky Next Expert View in Schritt 14 ausfüllen.

11. Wechseln Sie im Anwendungsmenü von Kaspersky Next Expert View zum Abschnitt **Authentifizierung** und geben Sie die URLs ein, die Sie in Schritt 4 aus Kaspersky Next Expert View kopiert haben:

    - Klicken Sie im Abschnitt **Web** auf die Schaltfläche **URI hinzufügen** und geben Sie die Anmelde-URL ein.
    - Geben Sie im Abschnitt **Front-Channel Abmelde-URL** die Front-Channel Abmelde-URL ein.

12. Wechseln Sie im Menü von Kaspersky Next Expert View zum Abschnitt **Zertifikate und Secrets** und gehen Sie anschließend wie folgt vor:

    a. Wechseln Sie zur Registerkarte **Client-Secrets** und klicken Sie auf Schaltfläche **Neuer geheimer Client Schlüssel**.

    b. Geben Sie im angezeigten Fenster eine Beschreibung für das Client-Secret an und wählen Sie anschließend einen Zeitraum aus, nach dem das Secret ablaufen soll.

    > Es wird empfohlen, das Ablaufdatum des Secrets auf beliebige Weise zu kopieren, um die Secrets rechtzeitig zu rotieren.

    a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

    Das erstellte Secret wird auf der Registerkarte **Client-Secrets** angezeigt.

    b. Kopieren Sie die Informationen aus der Spalte **Wert**.

    > Es wird dringend empfohlen, diese Informationen sofort nach der Erstellung des Client-Secrets zu kopieren.

13. Wechseln Sie im Menü von Kaspersky Next Expert View zum Abschnitt **Token-Konfiguration** und gehen Sie anschließend wie folgt vor:

    - Fügen Sie den optionalen Claim **onprem_sid** hinzu:

      a. Klicken Sie auf die Schaltfläche **Optionalen Claim hinzufügen**.

      b. Wählen Sie im angezeigten Fenster **ID** als Tokentyp aus und aktivieren Sie anschließend in der Spalte **Claim** das Kontrollkästchen neben **onprem_sid**.

      c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

    Der optionale Claim **onprem_sid** wird auf der Seite **Optionale Claims** angezeigt.

- Fügen Sie den optionalen Claim **preferred_username** hinzu:

  a. Klicken Sie auf die Schaltfläche **Optionalen Claim hinzufügen**.

  b. Wählen Sie im angezeigten Fenster **Access** als Tokentyp aus und aktivieren Sie anschließend in der Spalte **Claim** das Kontrollkästchen neben **onprem_sid**.

  c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

  Der optionale Claim **preferred_username** wird auf der Seite **Optionale Claims** angezeigt.

14. Wechseln Sie im Menü von Kaspersky Next Expert View zum Abschnitt **API-Berechtigungen** und fügen Sie die Berechtigungen hinzu:

    - **User.Read.All**
    - **User.Export.All**
    - **GroupMember.Read.All**
    - **Directory.Read.All**

    So fügen Sie eine Berechtigung hinzu:

    a. Klicken Sie auf die Schaltfläche **Berechtigung hinzufügen** und wählen Sie anschließend die Registerkarte **Microsoft-APIs** aus.

    b. Wählen Sie **Microsoft Graph** → **Anwendungsberechtigungen** und anschließend die Berechtigung aus, die Sie hinzufügen möchten.

    c. Klicken Sie auf die Schaltfläche **Berechtigung hinzufügen**.

    Die vier Berechtigungen werden hinzugefügt und auf der Seite **Konfigurierte Berechtigungen** angezeigt.

    d. Klicken Sie auf **Administratoreinwilligung erteilen für <tenant_name>** und klicken Sie anschließend im neuen Fenster auf **Ja**, um die Erteilung der Einwilligung zu den hinzugefügten Berechtigungen zu bestätigen.

15. Kehren Sie zurück zu Kaspersky Next Expert View und füllen Sie auf der Registerkarte **Allgemein** die folgenden Pflichtfelder aus:

    - **Mandanten-ID**. Die **Verzeichnis-ID (Mandant)**, die Sie in Schritt 10 kopiert haben.
    - **Client-ID**. Die **Anwendungs-ID (Client)** die Sie in Schritt 10 kopiert haben.
    - **Client-Secret**. Der Wert, den Sie in Schritt 12 kopiert haben.

16. Klicken Sie auf die Schaltfläche **Verbindung prüfen**, um zu überprüfen, ob die Einstellungen korrekt sind. Nachdem anschließend der Status **Verbunden** angezeigt wird, klicken auf die Schaltfläche **Speichern**.

Die Integrationseinstellungen werden gespeichert und die Integration mit der Microsoft Entra ID ist konfiguriert.

Sicherstellen, dass die Benutzer hinzugefügt werden

Nachdem Sie die Integration mit Microsoft Entra ID konfiguriert haben, müssen Sie Folgendes tun:

1. Wechseln Sie im Hauptmenü von Kaspersky Next Expert View zu **Benutzer und Rollen → Benutzer und Gruppen**, um sicherzustellen, dass die Benutzer und Gruppen aus Microsoft Entra ID zu Kaspersky Next Expert View hinzugefügt werden.

   Wenn die Benutzer und Gruppen in Ihrem Mandanten von Microsoft Entra ID aus dem Active Directory Ihres Unternehmens synchronisiert werden und die Abfrage des Active Directory konfiguriert ist, werden die Benutzer und Gruppen bereits als Ergebnis der Abfrage des Active Directory zu Kaspersky Next Expert View hinzugefügt.

   Andernfalls müssen Sie die Abfrage von Microsoft Entra ID aktivieren und ausführen, um die Benutzer und Gruppen aus Ihrem Mandanten von Microsoft Entra ID zu Kaspersky Next Expert View hinzuzufügen.

2. Weisen Sie den Benutzern und Gruppen die erforderlichen Rollen zu.

   Um einem Benutzer auf einem virtuellen Administrationsserver eine Rolle zuzuweisen, wechseln Sie im Hauptmenü zu **Benutzer und Rollen → Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus. Wenn Sie die Registerkarte **Gruppen** auswählen und anschließend der Gruppe, in welcher sich der Benutzer befindet, Rollen zuweisen, kann sich der Benutzer nicht an Kaspersky Security Center Cloud Console anmelden.

3. Senden Sie die Anmelde-URL, die Sie in Schritt 4 kopiert haben, an die Benutzer. Diese geben diese URL ein, um sich **mit ihren Anmeldedaten für Microsoft Entra ID im Arbeitsbereich von Kaspersky Next Expert View anzumelden**.

   Wenn sich der Benutzer von dem Benutzerkonto in Microsoft Entra ID abmeldet, das für die Authentifizierung in Kaspersky Next Expert View verwendet wurde und Kaspersky Next Expert View auf einer anderen Registerkarte oder in einem anderen Fenster desselben Browsers geöffnet ist, wird diese Sitzung für Kaspersky Next Expert View ebenfalls beendet und der Benutzer meldet sich automatisch von der Konsole ab.

   Wenn Kaspersky Next Expert View in einem anderen Browser oder auf verschiedenen Geräten geöffnet ist, wird diese Sitzung fortgesetzt, wenn sich der Benutzer von dem Benutzerkonto in Microsoft Entra ID abmeldet.

Um sich mit den Anmeldedaten für das Benutzerkonto von Microsoft Entra ID bei Kaspersky Next Expert View anzumelden, müssen sich die Benutzer an ihrem Benutzerkonto von Microsoft Entra ID anmelden können.

Beschränkungen

Wenn Sie sich mit den Anmeldeinformationen der Microsoft Entra ID in Kaspersky Next Expert View anmelden, gelten die folgenden Einschränkungen:

- Der Abschnitt „**Data Discovery**“ im Hauptmenü ist nicht verfügbar.
- Der Eintrag **Benutzerkonto verwalten** ist im oberen Bereich nicht verfügbar.
- Sie können nicht zwischen Arbeitsbereichen wechseln.

Aktivieren der Microsoft Entra ID-Abfrage

Um die Benutzer Ihres Microsoft Entra ID zu Kaspersky Next Expert View hinzuzufügen, müssen Sie die Microsoft Entra ID-Abfrage aktivieren.

So aktivieren Sie die Microsoft Entra ID-Abfrage:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Microsoft Entra ID** aus.
3. Aktivieren Sie im Abschnitt **Benutzer finden** den Umschalter **Abfrage von Microsoft Entra ID**.
4. Wenn Sie den standardmäßigen Abfragezeitplan ändern möchten, klicken Sie auf die Schaltfläche **Zeitplaneinstellungen**, geben Sie im angezeigten Fenster die Häufigkeit und Uhrzeit der Abfrage an und klicken Sie auf die Schaltfläche **Speichern**.

   Die Microsoft Entra ID-Abfrage wird gemäß dem von Ihnen konfigurierten Zeitplan ausgeführt.

5. Wenn Sie die Microsoft Entra ID-Abfrage sofort ausführen möchten, klicken Sie auf die Schaltfläche **Jetzt ausführen**.

   Die Benutzer werden geladen. Wenn die Benutzer geladen sind, ist die Microsoft Entra ID-Abfrage abgeschlossen.

6. Klicken Sie auf **Speichern**.

Die Microsoft Entra ID-Abfrage ist abgeschlossen und die Benutzer Ihres Microsoft Entra ID wurden zur Kaspersky Next Expert View hinzugefügt.

Kaspersky Next Expert View zur Liste mit Programmen hinzufügen

Sie können Benutzern erlauben, Kaspersky Next Expert View zu öffnen, indem sie in der Liste der Programme auf dessen Namen klicken, anstatt die Anmelde-URL einzugeben. Die Liste der Programme ist sowohl unter Meine Apps als auch im Launcher von Office 365 verfügbar.

So fügen Sie Kaspersky Next Expert View zur Liste der Programme hinzu:

1. Wechseln Sie im Hauptmenü des Microsoft Entra Admin Center zu **Identität** → **Anwendungen** → **App-Registrierungen** und wählen Sie anschließend auf der Registerkarte **Alle Anwendungen** die Instanz von Kaspersky Next Expert View aus, die Sie im Vorfeld in Microsoft Entra ID registriert haben.

2. Wählen Sie im Menü von Kaspersky Next Expert View den Abschnitt **Branding und Eigenschaften** und gehen Sie anschließend wie folgt vor:

   a. Geben Sie im Feld **URL der Startseite** die Anmelde-URL ein.

   b. Fügen Sie bei Bedarf im Feld **Neues Logo hochladen** ein Bild hinzu, das als Programmsymbol in der Liste der Programme angezeigt werden soll.

   c. Klicken Sie auf **Speichern**.

3. Wechseln Sie im Hauptmenü des Microsoft Entra Admin Center zu **Identität** →**Anwendungen** → **Unternehmensanwendungen** und wählen Sie Kaspersky Next Expert View.

   Die Seite mit der Programmübersicht wird geöffnet.

4. Wählen Sie im Menü von Kaspersky Next Expert View den Abschnitt **Eigenschaften** und gehen Sie anschließend wie folgt vor:

   a. Setzen Sie die folgenden Optionen auf **Ja**:

   - **Aktiviert für Benutzer zur Anmeldung?**

     Diese Aktion ist nur dann erforderlich, wenn für diese Option nicht standardmäßig **Ja** angegeben ist.

   - **Für Benutzer sichtbar?**

   b. Klicken Sie auf **Speichern**.

5. Wählen Sie im Menü von Kaspersky Next Expert View den Abschnitt **Benutzer und Gruppen** und gehen Sie anschließend wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Benutzer/Gruppe hinzufügen** und anschließend auf den Link unterhalb von **Benutzer und Gruppen**.

   b. Wählen Sie im neuen Fenster die Benutzer und Gruppen aus und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Das Fenster wird geschlossen.

   c. Klicken Sie auf die Schaltfläche **Zuweisen**.

Kaspersky Next Expert View ist für die ausgewählten Benutzer unter Meine Apps und im Launcher von Office 365 verfügbar. Die Benutzer können Kaspersky Next Expert View öffnen, ohne vorher die Anmelde-URL eingeben zu müssen, indem die Benutzer in der Liste der Programme auf den Namen klicken.

Benutzer zu Gerätebesitzern ernennen

Weitere Informationen, wie man einen Benutzer zum Gerätebesitzer macht, entnehmen Sie der Hilfe von Kaspersky Security für mobile Endgeräte.

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 **Asset-Verwaltung** → **Assets (Geräte)** ausgeführt werden: Klicken Sie auf den Namen des Geräts, das Sie zuweisen möchten, und klicken Sie dann auf den Link **Gerätebesitzer verwalten**.

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 Next Expert View 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.

Der Benutzer wird als Gerätebesitzer registriert.

Umgang mit Objekt-Revisionen

Der Abschnitt enthält Informationen über die Arbeit mit den Revisionen des Objekts. Kaspersky Next Expert View ermöglicht Ihnen, die Änderungen von Objekten nachzuverfolgen. Jedes Mal, wenn Sie die Änderungen des Objektes speichern, wird eine *Revision* erstellt. Jede Revision hat eine Nummer.

Folgende Objekte 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 Next Expert View, 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 neuen Fenster einen Text zur Beschreibung der Revision ein.

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. 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.

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 Nummer der 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.

Revision einer Richtlinie anzeigen und speichern

In Kaspersky Next Expert View 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 **Asset-Verwaltung** → **Richtlinien**.
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 Größe der Revision 10 MB überschreitet, können Sie diese in der Kaspersky Next Expert View 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.

Für die Richtlinien von Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Security for Mac enthält der Bericht keine Informationen über die Richtlinienprofile.

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.

Bei Bedarf können Sie Richtlinienrevisionen vergleichen. Diese Option ist für die Richtlinien der folgenden Komponenten verfügbar: Administrationsserver, Administrationsagent, Kaspersky Endpoint Security für Windows (beginnend ab Version 14.0 des Web-Plug-ins) und Kaspersky Endpoint Security for Mac (beginnend ab Version 12.2.1 Patch A des Web-Plug-ins).

Richtlinienrevisionen vergleichen

Sie haben die folgenden Vergleichsmöglichkeiten: Vergleich von früheren Revisionen einer Richtlinie mit der aktuellen Version, Vergleich verschiedener in der Liste ausgewählter Revisionen untereinander und Vergleich einer Revision einer Richtlinie mit einer Revision einer anderen Richtlinie. Die Optionen sind für Richtlinien der folgenden Komponenten verfügbar: Administrationsserver, Administrationsagent, Kaspersky Endpoint Security für Windows (beginnend ab Version 14.0 des Web-Plug-ins) und Kaspersky Endpoint Security for Mac (beginnend ab Version 12.2.1 Patch A des Web-Plug-ins).

So zeigen Sie eine Richtlinienrevision an:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf die Richtlinie, deren Revisionen Sie vergleichen möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.
3. Wechseln Sie zur Registerkarte **Revisionsverlauf** und aktivieren Sie die Kontrollkästchen neben den zu vergleichenden Versionen.
4. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Vergleichen** und wählen Sie anschließend eine der folgenden Optionen aus der Dropdown-Liste:

   - **Mit aktueller Revision**, wenn Sie die in Schritt 3 ausgewählte Revision mit der zuletzt gespeicherten Revision der gleichen Richtlinie vergleichen möchten.
   - **Ausgewählte Revisionen**, wenn Sie die zwei Revisionen vergleichen möchten, deren Kontrollkästchen Sie in Schritt 3 aktiviert haben.

     Die Reihenfolge, in der die Kontrollkästchen aktiviert werden, hat keinen Einfluss auf das Vergleichsergebnis. Standardmäßig wird die frühere Revision der ausgewählten Revision mit der neuesten Revision verglichen. Wenn Sie beispielsweise die Kontrollkästchen neben den Revisionen 5 und 1 auswählen, wird Revision 1 mit Revision 5 verglichen. Der Bericht enthält Informationen über jene Einstellungen in Revision 1, die im Vergleich zu Revision 5 hinzugefügt, entfernt oder geändert wurden.
   - **Mit anderer Richtlinienrevision**, wenn Sie die Revisionen von zwei verschiedenen Richtlinien vergleichen möchten.

Führen Sie im neu geöffneten rechten Bereich Folgendes aus:

a. Wählen Sie im Feld **Anwendungsname** die Richtlinie aus, die Sie vergleichen möchten: Administrationsagent oder Administrationsserver.

b. Geben Sie im Feld **Richtlinienname** den Namen der Richtlinie an, deren Revision Sie mit der in Schritt 3 ausgewählten Revision vergleichen möchten.

Die Liste der Richtlinienrevisionen wird angezeigt.

c. Wählen Sie die erforderliche Revision aus und klicken Sie auf die Schaltfläche **Vergleichen**.

In einem neuen Tab Ihres Browsers wird ein Bericht über den Revisionsvergleich im HTML-Format angezeigt.

Wenn das Ergebnis des Vergleichs 10 MB überschreitet, wird ein entsprechender Dialog angezeigt. Sie können entweder auf die Schaltfläche **Als Datei speichern** klicken, um den Bericht als Datei zu speichern, oder den Vorgang abbrechen.

Der Bericht wird in der Sprache angezeigt, die in der Benutzeroberfläche Ihrer Kaspersky Next Expert View verwendet wird. Sie können einzelne Abschnitte des Berichts erweitern, indem Sie auf das Symbol mit dem Pfeil nach unten (▼) neben dem Abschnitt klicken. Durch Anklicken des Symbols mit dem Pfeil nach oben (▲) können Sie erweiterte Abschnitte wieder ausblenden.

Der Bericht enthält die folgenden Informationen:

- Kaspersky-Logo.
- Den Namen des Berichts.
- Die Uhrzeit und das Datum der Berichtserstellung.
- Den Richtliniennamen, den Administrationsserver und die Administrationsgruppe, welche die Richtlinie bzw. die Richtlinien, deren Revisionen verglichen werden, enthalten.
- Die Schaltfläche **Als HTML speichern**. Wenn Sie diese Schaltfläche anklicken, wird der Bericht auf Ihrem Computer gespeichert.
- Den Abschnitt **Zusammenfassung**, der die allgemeinen Informationen zu den verglichenen Revisionen anzeigt: Name der Richtlinie bzw. der Richtlinien, Nummer der Revision, Uhrzeit und Datum der gespeicherten Revision, Benutzer der gespeicherten Revision und Beschreibung zur Revision.

  Für geerbte Richtlinien wird kein Benutzer angezeigt.

- Unterschiede zwischen den verglichenen Revisionen. Die Unterschiede werden in den folgenden Abschnitten dargestellt:
  - **Hinzugefügte Einstellungen**
  - **Entfernte Einstellungen**
  - **Geänderte Einstellungen**

- **Einstellungen, die nur für Objekt 1 verfügbar sind** (Wenn Sie die Revisionen zweier verschiedener Richtlinien verglichen haben)
- **Einstellungen, die nur für Objekt 2 verfügbar** sind (Wenn Sie die Revisionen zweier verschiedener Richtlinien verglichen haben)

Wenn ein Abschnitt keine Daten enthält, wird er nicht angezeigt.

Für die Richtlinien von Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Security for Mac enthält der Bericht über den Revisionsvergleich keine Informationen über die Richtlinienprofile.

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-Anwendungen auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. KSN ermöglicht den Abruf von Informationen über die auf den verwalteten Client-Geräten installierten Programme aus den Kaspersky-Reputations-Datenbanken.

Wenn Sie an KSN teilnehmen, stimmen Sie zu, dass Informationen über die Ausführung der auf den Client-Geräten installierten Kaspersky-Anwendungen, die von Kaspersky Next Expert View 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.

Die Anwendung fordert Sie auf, während der Ausführung des Schnellstartassistenten eine Verbindung mit 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 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 vorherigen Version der KSN-Erklärung, die Sie zuvor akzeptiert haben.

Wenn KSN aktiviert ist, prüft Kaspersky Next Expert View, ob auf die KSN-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung 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 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.

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 ausgeführt.

KSN aktivieren und deaktivieren

Um KSN zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Einstellungen** aus.

3. Stellen Sie den Umschalter auf die Position **Kaspersky Security Network verwenden Aktiviert**.

   KSN ist aktiviert.

   Wenn dieser Umschalter aktiviert ist, senden Client-Geräte die Ergebnisse der Patch-Installation an Kaspersky. Wenn Sie den Umschalter aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Um die KSN zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Einstellungen** aus.

3. Stellen Sie den Umschalter auf die Position **Kaspersky Security Network verwenden Deaktiviert**.

   KSN ist deaktiviert.

   Wenn der Umschalter deaktiviert ist, werden von den Client-Geräten keine Ergebnisse über die Installation von Patches an Kaspersky übermittelt.

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 auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Einstellungen**.

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. Wenn die KSN-Erklärung aktualisiert wurde, wird sie beim Öffnen der Kaspersky Next Expert View automatisch angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, werden Sie KSN weiterhin gemäß der Version der KSN-Erklärung verwenden, die Sie zuvor akzeptiert haben. Sie können die aktualisierte KSN-Erklärung später anzeigen und akzeptieren.

So können Sie die KSN-Erklärung anzeigen und anschließend akzeptieren oder ablehnen:

1. Klicken Sie auf den Link **Benachrichtigungen anzeigen** in der oberen rechten Ecke des Hauptanwendungsfensters.

   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.

Löschen von Objekten

Sie können Objekte löschen, einschließlich der folgenden:

- Richtlinien
- Aufgaben
- Installationspakete
- Virtuelle Administrationsserver
- Benutzer

- Sicherheitsgruppen
- Administrationsgruppen

Wenn Sie ein Objekt löschen, verbleiben die Informationen darüber in der Datenbank. Die Speicherdauer für Informationen über die gelöschten Objekte ist identisch mit der Speicherdauer für Revisionen des Objekts (die empfohlenen Dauer beträgt 90 Tage). Sie können die Speicherdauer nur ändern, wenn Sie über die Berechtigung **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 Administrationsagent und alle weiteren Kaspersky-Sicherheitsanwendungen, bspw. Kaspersky Endpoint Security, auf dem Gerät.

Kaspersky Next Expert View verarbeitet die Geräte in der Gruppe "Nicht zugeordnete Geräte" gemäß den folgenden Regeln:

- 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 Geräteaufbewahrungsregeln wirken sich nicht auf Geräte aus, bei denen mindestens ein Laufwerk mittels BitLocker-Laufwerkverschlüsselung verschlüsselt ist. 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 beim Löschen solcher Geräte (entweder aus der Gruppe **Nicht zugeordnete Geräte** oder aus der Gruppe **Verwaltete Geräte**) öffnet, das Kontrollkästchen **Ich kenne das Risiko und möchte die 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 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 anschließend weiterhin für den Administrationsserver sichtbar ist und Sie eine regelmäßige Netzwerkabfrage konfiguriert haben, erkennt Kaspersky Next Expert View das Gerät während der Netzwerkabfrage erneut und fügt es wieder 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.

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 von Kaspersky Next Expert View 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: Regelmäßige Aktualisierung der Kaspersky-Datenbanken und -Programme

Dieser Abschnitt enthält ein Szenario zum regelmäßigen Update der Kaspersky-Datenbanken, Softwaremodule und Programme. Nachdem Sie das Szenario zum Konfigurieren des Netzwerkschutzes abgeschlossen haben, müssen Sie die Zuverlässigkeit des Schutzsystems sicherstellen. Durch diese Wartung wird sichergestellt, dass der Schutz der verwalteten Geräte vor einer Reihe von Bedrohungen, einschließlich Viren, Netzwerkangriffen und Phishing-Angriffen, gewährleistet bleibt.

Es existieren verschiedene Schemen die Sie nutzen können, um Updates für die Komponenten von Kaspersky Next Expert View und Sicherheitsanwendungen zu installieren. Wählen Sie ein oder mehrere Schemen, welche die Anforderungen Ihres Netzwerks am besten erfüllen.

Das folgende Szenario beschreibt das Update-Schema, bei dem Aktualisierungen in die Datenverwaltungen der Verteilungspunkte heruntergeladen werden. Wenn die verwalteten Geräte nicht mit den Verteilungspunkten verbunden sind, erwägen Sie, das Update der Datenbanken von Kaspersky, der Programm-Module und der Programme manuell oder direkt von einem Kaspersky-Update-Server durchzuführen.

Wenn Sie dieses Szenario abschließen, treten die folgenden Ergebnisse auf:

- Komponenten von Kaspersky Next Expert View werden automatisch oder nur dann aktualisiert, wenn Sie den Status *Genehmigt* für die Updates festlegen.
- Kaspersky-Sicherheitsanwendungen, Kaspersky-Datenbanken und Softwaremodule werden nach dem von Ihnen festgelegten Zeitplan aktualisiert. Standardmäßig installieren Kaspersky-Sicherheitsanwendungen nur die Updates, die Sie genehmigen.

Sie können den Update-Prozess so konfigurieren, dass Updates auf zwei Arten heruntergeladen und installiert werden:

- Automatisch

  In diesem Fall müssen Sie dieses Szenario nur einmal ausführen. Sie müssen einen Zeitplan für die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* (falls vorhanden) und für die Update-Aufgaben der Kaspersky-Sicherheitsanwendungen festlegen und die standardmäßigen Update-Einstellungen beibehalten, die in den Einstellungen des Administrationsagenten angegeben sind.

- Manuell

  Sie können den Update-Prozess so konfigurieren, dass die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* (falls vorhanden) und die Update-Aufgaben für die Kaspersky-Sicherheitsanwendungen manuell ausgeführt werden. Sie können den Administrationsagenten auch so konfigurieren, dass Updates für die Komponenten von Kaspersky Next Expert View nur installiert werden, wenn Sie den Status *Genehmigt* für die Updates festlegen.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

1. die Sicherheitsanwendungen von Kaspersky gemäß dem Szenario zur Verteilung von Kaspersky-Anwendungen via Kaspersky Next Expert View auf den verwalteten Geräten verteilt haben und Wenn Sie dieses Szenario ausführen, haben Sie in Übereinstimmung mit der Anzahl der verwalteten Geräte und der Netzwerktopologie eine geeignete Anzahl an Verteilungspunkten zugewiesen.

2. alle notwendigen Richtlinien, Richtlinienprofile und Aufgaben entsprechend dem Szenario "Konfiguration des Netzwerkschutzes" konfiguriert haben.

Schritte

Die Konfiguration der regelmäßigen Updates von Kaspersky-Datenbanken und -Programmen erfolgt schrittweise:

1. **Erstellen der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte**

   Erstellen der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*. Beim Ausführen dieser Aufgabe lädt Kaspersky Next Expert View die Updates mithilfe der Aufgabe für die Verteilungspunkte direkt von den Kaspersky-Update-Servern herunter.

   Anleitung: Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

2. **Konfigurieren der Verteilungspunkte**

   Stellen Sie sicher, dass die Option **Aktiviert** in den Einstellungen aller benötigten Verteilungspunkten aktiviert ist. Wenn diese Option für einen Verteilungspunkt deaktiviert ist, können die zum Lieferumfang des Verteilungspunkts gehörenden Geräte Updates nur von einer lokalen Ressource oder direkt von Kaspersky Update-Servern herunterladen.

   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.

3. **Optimieren des Update-Prozesses durch Diff-Dateien (optional)**

   Die Aktivierung dieser Funktion resultiert in einem verringerten Datenverkehr zwischen den Verteilungspunkten und den verwalteten Geräten. Um diese Funktion zu nutzen, aktivieren Sie die Option **Diff-Dateien herunterladen** in den Eigenschaften der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*.

   Anleitung: Diff-Dateien zum Update von Kaspersky-Datenbanken und Programm-Modulen verwenden

4. **Zu installierende Updates festlegen**

   Standardmäßig besitzen heruntergeladene Software-Updates den Status *Nicht definiert*. Ändern Sie den Status in *Genehmigt* oder in *Abgelehnt* um festzulegen, ob dieses Update auf Netzwerkgeräten installiert werden soll. Genehmigte Updates werden immer installiert. Die nicht definierten Updates können nur in Übereinstimmungen mit den Richtlinieneinstellungen des Administrationsagenten auf dem Administrationsagenten und auf anderen Komponenten von Kaspersky Next Expert View installiert werden. Updates, für die Sie den Status *Abgelehnt* gewählt haben, werden auf den Geräten nicht installiert.

   Anleitung:

   - Informationen zum Update-Status
   - Genehmigen und Ablehnen von Software-Updates

5. **Konfiguration der automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Next Expert View**

   Standardmäßig werden die heruntergeladenen Updates und Patches für den Administrationsagenten und andere Komponenten von Kaspersky Next Expert View 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: Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Next Expert View aktivieren und deaktivieren

6. **Konfiguration der automatischen Installation von Updates für die Sicherheitsanwendungen**

   Erstellen Sie die Update-Aufgaben für verwaltete Programme, um zeitnahe Updates für die Anwendungen, Programm-Module und Kaspersky-Datenbanken (einschließlich der Antiviren-Datenbanken) zu gewährleisten. Wir empfehlen, dass Sie beim Konfigurieren des Aufgabenplans, die Option **Nach dem Download von Updates in die Datenverwaltung** aktivieren. Dadurch wird sichergestellt, dass neue Updates so schnell wie möglich installiert werden.

   Standardmäßig werden Updates für die verwalteten Programme erst installiert, nachdem Sie den Update-Status in *Genehmigt* geändert haben. In Kaspersky Endpoint Security für Windows können Sie die Update-Einstellungen in der Update-Aufgabe 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: Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren

7. **Updates für verwaltete Kaspersky-Anwendungen genehmigen und ablehnen**

   Standardmäßig besitzen heruntergeladene Programm-Updates den Status *Nicht definiert*. Sie können den Status auf *Genehmigt* oder *Abgelehnt* ändern. Genehmigte Updates werden immer installiert. Wenn ein Update für eine verwaltete Kaspersky-Anwendung das Überprüfen und Akzeptieren des Endbenutzer-Lizenzvertrags erfordert, müssen Sie die Bestimmungen zuvor akzeptieren. Danach kann das Update an die verwalteten Geräte verteilt werden. Updates, für die Sie den Status *Abgelehnt* gewählt haben, werden auf den Geräten nicht installiert. Wenn ein abgelehntes Update für eine verwaltete Anwendung bereits zuvor installiert wurde, wird Kaspersky Next Expert View 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. Ein nahtloses Update der folgenden Komponenten wird nicht unterstützt: Administrationsserver, Kaspersky Next Expert View und Web-Plug-ins zur Verwaltung.

Anleitung: Genehmigen und Ablehnen von Software-Updates

Nach Abschluss des Szenarios können Sie mit der Überwachung des Netzwerkstatus fortfahren.

Informationen zum Aktualisieren von Kaspersky-Datenbanken, Softwaremodulen und Anwendungen

Um sicherzustellen, dass der Schutz Ihrer 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 Next Expert View, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung 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 von Kaspersky Next Expert View und der Sicherheitsanwendungen

  Kaspersky-Experten führen alle erforderlichen Updates für Kaspersky Next Expert View und seine Komponenten sowie für verwaltete Kaspersky-Anwendungen durch. Sie können diese Updates nicht selbst durchführen.

Abhängig von der Konfiguration Ihres Netzwerks können die folgenden Verfahren zum Herunterladen und Verteilen der erforderlichen Updates auf die verwalteten Geräte verwendet werden:

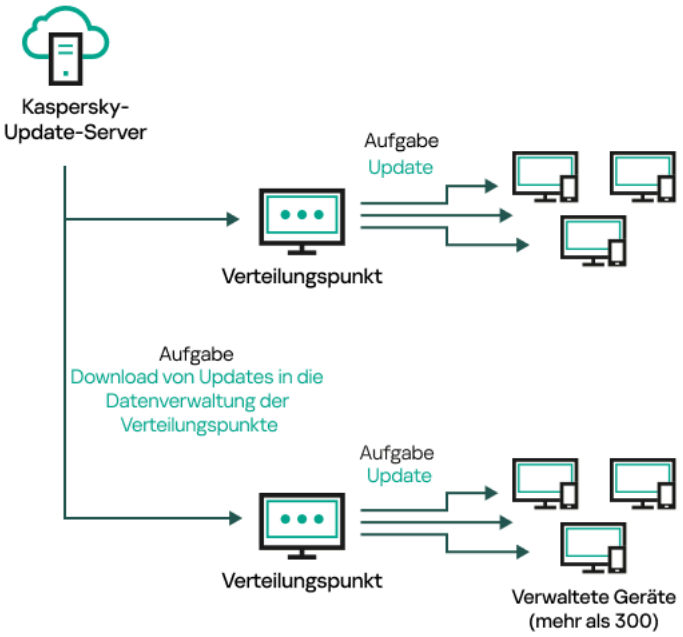
- Verwenden der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*
- Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server
- Direkt von den Kaspersky Update-Servern zu Sicherheitsanwendungen auf den verwalteten Geräten

Verwenden der Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

In diesem Schema lädt Kaspersky Next Expert View über die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* Updates herunter. Die verwalteten Geräte, die zum Umfang eines Verteilungspunkts gehören, laden die Updates aus der Datenverwaltung des Verteilungspunkts herunter (siehe Abbildung unten).

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.



Aktualisierung mit Hilfe der Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

Wenn die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* abgeschlossen ist, werden die folgenden Updates in die Datenverwaltung der Verteilungspunkte heruntergeladen:

- 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 die Komponenten von Kaspersky Next Expert View

  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 werden über die Update-Aufgabe installiert und können in den Eigenschaften dieser Aufgabe konfiguriert werden.

Jede Anwendung von Kaspersky fordert die erforderlichen Updates vom Administrationsserver an. Der Administrationsserver aggregiert diese Anforderungen und lädt nur die Updates in die Datenverwaltungen der Verteilungspunkte herunter, die von einem Programm 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 *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* der Administrationsserver die folgenden Informationen automatisch an Kaspersky-Update-Server, um das Herunterladen von relevanten Versionen der Kaspersky-Datenbanken und Programm-Module sicherzustellen:

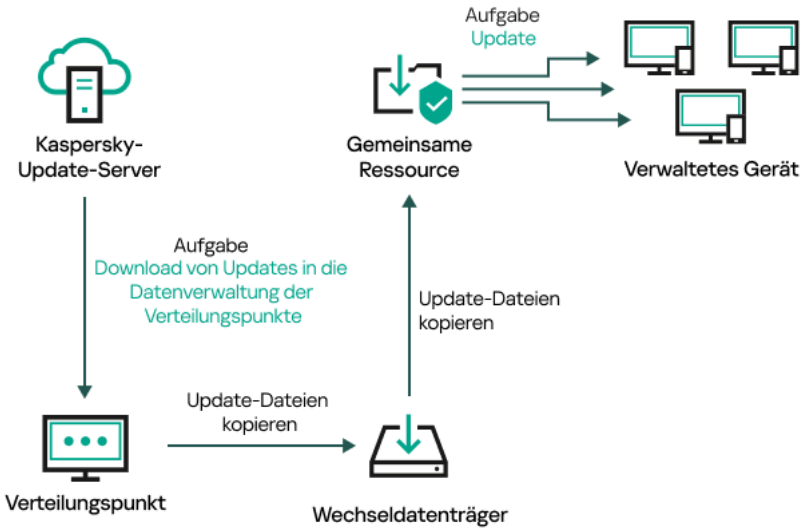
- Anwendungs-ID und Version des Programms
- ID der Programminstallation

- ID des aktiven Schlüssels
- Ausführungs-ID der Aufgabe herunter

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.

Über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

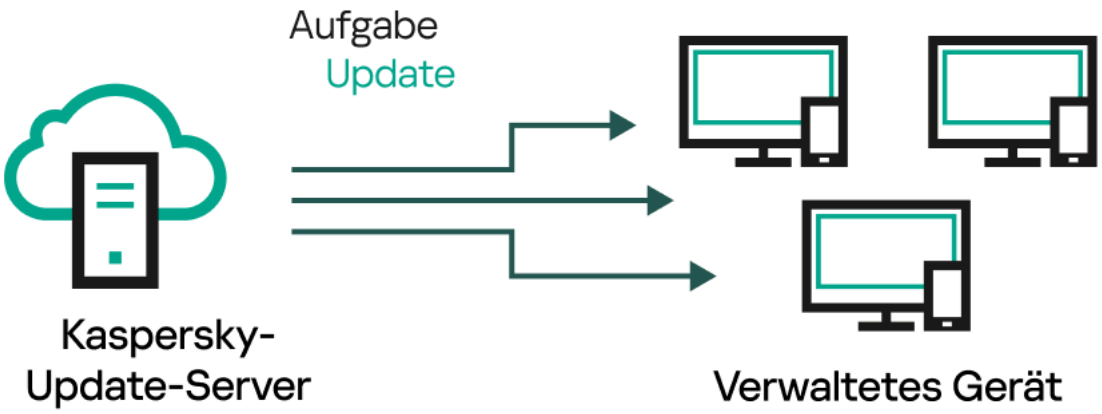
Wenn die Client-Geräte keine Verbindung zu einem Verteilungspunkt haben, können ein lokaler Ordner oder eine freigegebene Ressource als Quelle für das Update von Kaspersky-Datenbanken, -Softwaremodulen und -Anwendungen verwendet werden. In diesem Schema werden die erforderlichen Updates aus der Datenverwaltung eines Verteilungspunkts auf einen Wechseldatenträger und anschließend in den lokalen Ordner oder die freigegebene Ressource kopiert, der bzw. die in den Einstellungen von Kaspersky Endpoint Security für Windows als Update-Quelle angegeben ist (siehe Abbildung unten).



Manuelles Upgrade über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Direkt von den Kaspersky Update-Servern zu Kaspersky Endpoint Security für Windows auf den verwalteten Geräten

Auf den verwalteten Geräten erhält Kaspersky Endpoint Security für Windows Updates direkt von den Kaspersky-Update-Servern (siehe Abbildung unten).



Updates von Sicherheitsanwendungen direkt von Kaspersky Update-Servern aus

In diesem Schema verwendet die Sicherheitsanwendung nicht die von Kaspersky Next Expert View 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. Die vollständige Beschreibung der Einstellungen finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

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 *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* für eine Administrationsgruppe anlegen. Diese Aufgabe wird für die Verteilungspunkte ausgeführt, die zur angegebenen Administrationsgruppe gehören.

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 Next Expert View-Komponenten
- Updates von Kaspersky-Sicherheitsanwendungen

Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

*So erstellen Sie die Aufgabe **Updates in die Datenverwaltung der Verteilungspunkte herunterladen** für eine ausgewählte Administrationsgruppe:*

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Aufgaben**.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Next Expert View 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 Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die standardmäßigen Aufgabeneinstellungen ändern. 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 **Anwendungseinstellungen** 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**

  Kaspersky Next Expert View lädt die Updates für Datenbanken und Programm-Module mittels eines neuen Schemas herunter. Damit das Programm 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** (Standardmäßig ausgewählt)

    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.

- **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 Next Expert View 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.

- **Monatlich am ausgewählten Tag**

  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. Dieser Parameter 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.

Verwaltete Geräte so konfigurieren, dass Updates nur von Verteilungspunkten empfangen werden

Verwaltete Geräte können Updates von Kaspersky-Datenbanken, Softwaremodulen und Kaspersky-Anwendungen aus verschiedenen Quellen abrufen: direkt von Update-Servern, von Verteilungspunkten, oder aus einem lokalen oder Netzwerkordner. Sie können Verteilungspunkte als einzige mögliche Quelle für Updates angeben.

So konfigurieren Sie verwaltete Geräte, sodass Updates nur von Verteilungspunkten empfangen werden:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf die Richtlinie für Administrationsagenten.
3. Wechseln Sie im Eigenschaftenfenster der Richtlinie zur Registerkarte **Anwendungseinstellungen**.
4. Schalten Sie im Abschnitt **Einstellungen** die Umschalttaste **Dateien nur über Verteilungspunkte übertragen** ein.
5. Aktivieren Sie das Schloss-Symbol (🔒) für diese Umschalttaste.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Richtlinie wird auf die ausgewählten Geräte angewendet, und die Geräte erhalten nur Updates von Verteilungspunkten.

Automatische Installation von Updates und Patches für die Komponenten von Kaspersky Next Expert View aktivieren und deaktivieren

Die automatische Installation der Patches für Komponenten von Kaspersky Next Expert View wird standardmäßig bei der Installation des Administrationsagenten auf dem Gerät aktiviert. Sie können sie bei der Installation des Administrationsagenten oder später mithilfe einer Richtlinie deaktivieren.

Um die automatische Installation der Patches für Komponenten von Kaspersky Next Expert View 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 Schritten des Assistenten.

   Auf dem Gerät wird der Administrationsagent mit der deaktivierten automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Next Expert View installiert. Sie können die automatische Installation später mithilfe einer der Richtlinie aktivieren.

Um die automatische Installation der Patches für Komponenten von Kaspersky Next Expert View 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. Wählen Sie im Eigenschaftenfenster die 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 Next Expert View installiert. Sie können die automatische Installation später mithilfe einer der Richtlinie aktivieren.

Wenn bei der Installation des Administrationsagenten auf dem Gerät das Kontrollkästchen in Schritt 4 aktiviert (deaktiviert) war, können Sie die automatische Installation später mithilfe einer Richtlinie des Administrationsagenten deaktivieren (aktivieren).

Um die automatische Installation der Patches für Komponenten von Kaspersky Next Expert View mithilfe einer Richtlinie des Administrationsagenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf die Richtlinie für Administrationsagenten.
3. Wählen Sie im Eigenschaftenfenster der Richtlinie die Registerkarte **Anwendungseinstellungen** aus.

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. Vergewissern Sie sich, dass (**Erzwingen**) das Symbol Schloss (🔒) für diese Umschalttaste aktiviert ist.

Die Richtlinie wird auf die ausgewählten Geräte angewendet und die automatische Installation von Updates und Patches für die Komponenten von Kaspersky Next Expert View 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 **Asset-Verwaltung** → **Aufgaben**.

2. Klicken Sie auf **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. Legen Sie die Administrationsgruppe, die Geräteauswahl oder die Geräte, für die Aufgabe gilt, fest.

7. Wenn Sie im Schritt **Erstellung der Aufgabe abschließen** die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die standardmäßigen Aufgabeneinstellungen ändern. 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. Definieren Sie auf der Registerkarte **Anwendungseinstellungen** im Aufgabeneigenschaftenfenster die Einstellungen der Update-Aufgabe im lokalen oder mobilen Modus:

    - **Lokaler Modus**: In den Einstellungen auf dieser Registerkarte wird festgelegt, wie das Gerät Updates erhält, wenn die Verbindung zwischen dem Gerät und dem Administrationsserver hergestellt wird.

    - **Mobiler Modus**: In den Einstellungen auf dieser Registerkarte wird festgelegt, wie das Gerät Updates empfängt, wenn keine Verbindung zwischen Kaspersky Next Expert View und dem Gerät hergestellt wird (z. B. wenn 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. Ändern Sie bei Bedarf die Positionen der Quellen in der Liste mit den Tasten **Nach oben** und **Nach unten**. Wenn mehrere Update-Quellen aktiviert sind, versucht Kaspersky Endpoint Security für Windows, sich nacheinander mit ihnen zu verbinden, beginnend am Anfang der Liste, und führt die Update-Aufgabe aus, indem es das Update-Paket von der ersten verfügbaren Quelle abruft.

    Wenn Kaspersky Next Expert View als Update-Quelle festgelegt ist, werden die Updates aus der Datenverwaltung eines Verteilungspunkts und nicht aus der Datenverwaltung des Administrationsservers heruntergeladen. Stellen Sie sicher, dass Sie Verteilungspunkte zugeordnet und die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* erstellt haben.

12. Aktivieren Sie die Option **Genehmigte Updates für Programm-Module installieren**, um die Updates für die Programm-Module einmalig von 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 Next Expert View 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.

Informationen zum Update-Status

Status ist ein Attribut von Softwareupdates, das angibt, ob ein bestimmtes Programm-Update auf einem Netzwerkgerät installiert werden muss.

Ein Update kann u. a. folgenden Status haben:

- *Nicht definiert*

  Standardmäßig besitzen heruntergeladene Software-Updates den Status *Nicht definiert*. Die nicht definierten Updates können nur in Übereinstimmungen mit den Richtlinieneinstellungen des Administrationsagenten auf dem Administrationsagenten und auf anderen Komponenten von Kaspersky Next Expert View installiert werden.

- *Genehmigt*

  Genehmigte Updates werden immer installiert. Wenn ein Update eine Überprüfung und ein Akzeptieren des Endbenutzer-Lizenzvertrags benötigt, müssen Sie die Bestimmungen zuerst akzeptieren.

- *Abgelehnt*

  Updates, für die Sie den Status *Abgelehnt* gewählt haben, werden auf den Geräten nicht installiert.

Sie können den Status von Updates für die folgende Software ändern:

- Administrationsagent und andere Komponenten von Kaspersky Next Expert View

  Standardmäßig werden die heruntergeladenen Updates und Patches für Komponenten von Kaspersky Next Expert View 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.

  Updates für Komponenten von Kaspersky Next Expert View können nicht deinstalliert werden, auch wenn Sie für eine Aktualisierung den Status *Abgelehnt* festlegen.

- Kaspersky-Sicherheitsanwendungen

  Standardmäßig werden Updates für die verwalteten Programme erst installiert, nachdem Sie den Update-Status in *Genehmigt* geändert haben. Wenn ein abgelehntes Update für eine Sicherheitsanwendung bereits zuvor installiert wurde, wird Kaspersky Next Expert View versuchen, dieses Update von allen Geräten zu deinstallieren.

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.

Das Genehmigen und Ablehnen von Updates ist nur für Administrationsagenten und verwaltete Anwendungen verfügbar, die auf Windows- oder Linux-basierten Client-Geräten installiert sind. Ein nahtloses Update der folgenden Komponenten wird nicht unterstützt: Administrationsserver, Kaspersky Next Expert View 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 → Kaspersky-Anwendungen → 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. Akzeptieren Sie gegebenenfalls die Lizenzverträge, indem Sie auf **Lizenzverträge anzeigen und akzeptieren** klicken.

   Um die von den Kaspersky-Anwendungen verarbeiteten Daten anzuzeigen, für die Sie nahtlose Updates genehmigen möchten, klicken Sie im geöffneten Bereich "Lizenzvertrag" auf **Liste der Daten anzeigen**.

3. Wählen Sie die Updates aus, die Sie genehmigen oder ablehnen möchten.

4. 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 Next Expert View 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.

Diff-Dateien zum Update von Kaspersky-Datenbanken und -Software-Modulen verwenden

Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Die Verwendung von Diff-Dateien schränkt den Datenverkehr in Ihrem Unternehmensnetzwerk ein, da Diff-Dateien weniger Platz einnehmen als die vollständigen Dateien der Datenbanken und Software-Module. Wenn die Funktion *Diff-Dateien herunterladen* auf einem Verteilungspunkt aktiviert ist, werden die Diff-Dateien auf diesem Verteilungspunkt gespeichert. So können Geräte, die Updates von 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 Verteilungspunkts, 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 Verteilungspunkt, von dem sie ihre Updates erhalten.

Verteilungspunkte verwenden kein IP-Multicast zur automatischen Verteilung von Diff-Dateien.

So aktivieren Sie die Funktion zum Download von Diff-Dateien:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Aufgaben**.
2. Klicken Sie auf die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*, um die Aufgabeneigenschaften zu öffnen.
3. Aktivieren Sie auf der Registerkarte **Anwendungseinstellungen** die Option **Diff-Dateien herunterladen**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

   Die Funktion zum Download von Diff-Dateien ist aktiviert. Diff-Dateien von Updates werden zusätzlich zu den Update-Dateien jedes Mal heruntergeladen, wenn die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* ausgeführt wird.

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.

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 der Verteilungspunkte.

Wenn Sie Updates von Datenbanken und Programm-Modulen auf einem Gerät (oder auf einer Gruppe von Geräten) durchführen müssen, die nicht mit 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 aus folgenden Quellen:

- Verteilungspunkt.

  Um sicherzustellen, dass die Datenverwaltung des Verteilungspunkts über die, von der auf dem Offline-Gerät installierten Sicherheitsanwendung benötigten, Updates verfügt, muss auf mindestens einem der verwalteten Online-Geräte im Bereich des Verteilungspunktes die gleiche Sicherheitsanwendung installiert sein. Die Anwendung muss so konfiguriert sein, dass sie die Updates aus der Datenverwaltung des Verteilungspunkts durch die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* erhält.

- Jedes Gerät, dass die gleiche Sicherheitsanwendung installiert und so konfiguriert hat, dass sie Updates aus der Datenverwaltung des Verteilungspunkts 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 Verteilungspunkts kopiert werden.

So aktualisieren Sie Kaspersky-Datenbanken und Programm-Module auf autonomen Geräten:

1. Schließen Sie den Wechseldatenträger am Verteilungspunktgerät an.

2. Kopieren Sie die Update-Dateien auf den Wechseldatenträger.

   Standardmäßig befinden sich die Updates unter: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.

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.

Verwalten von Programmen von Drittanbietern auf Client-Geräten

In diesem Abschnitt werden die Funktionen von Kaspersky Next Expert View für die Verwaltung von Programmen von Drittanbietern beschrieben, die auf Client-Geräten installiert sind.

Einschränkungen des Schwachstellen- und Patch-Managements

Die Funktion "Schwachstellen- und Patch-Management" weist einige Einschränkungen auf, die davon abhängig sind, welche Lizenz Sie verwenden und in welchem Modus Kaspersky Next Expert View ausgeführt wird.

Die folgenden Lizenzen unterstützen die Funktion "Schwachstellen- und Patch-Management" nicht:

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

Die folgenden Lizenzen unterstützen die Funktion "Schwachstellen- und Patch-Management":

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Enterprise

Die untere Tabelle stellt die Beschränkungen von Kaspersky Next Expert View im Testmodus, unter einer Lizenz, die das Schwachstellen- und Patch-Management nicht unterstützt, und unter einer Lizenz, die das Schwachstellen- und Patch-Management unterstützt, gegenüber.

Einschränkungen des Schwachstellen- und Patch-Managements

Beschränkungen	Testmodus	Kommerzieller Modus: Lizenzen, die das Schwachstellen- und Patch-Management nicht unterstützen	Kommerzieller Modus: Lizenzen, die das Schwachstellen- und Patch-Management unterstützen
Maximale Anzahl an Aufgaben vom Typ *Windows-Updates installieren* oder vom Typ *Schwachstellen schließen*	4	4	0 (Es können keine neuen Aufgaben diesen Typs erstellt werden)
Maximale Anzahl an Aufgaben vom Typ *Erforderliche Updates installieren und Schwachstellen schließen*	2	Nicht unterstützt	4
Maximale Anzahl an Regeln in allen Aufgaben vom Typ *Erforderliche Updates installieren und Schwachstellen schließen*	10	Nicht unterstützt	50
Maximale Anzahl an Programm-Updates, die gleichzeitig den Status *Genehmigt* besitzen können (über alle Server, einschließlich virtueller)	100	Nicht unterstützt	1.000

Maximale Anzahl an Programm-Updates, die einer Aufgabe manuell hinzugefügt werden können (über alle Server, einschließlich virtueller)	500	1.000	1.000
Maximale Anzahl von Programm-Schwachstellen, die einer Aufgabe manuell hinzugefügt werden können (über alle Server, einschließlich virtueller)	500	1.000	1.000

Verfügbarkeit der Funktionen von Schwachstellen- und Patch-Management im Test- und kommerziellen Modus sowie unter verschiedenen Lizenzoptionen

Die Verfügbarkeit der Funktionen des Schwachstellen- und Patch-Managements hängt in der Kaspersky Next Expert View davon ab, ob Sie diese im Test- oder kommerziellen Modus verwenden, sowie von der von Ihnen ausgewählten Lizenzoption. Verwenden Sie die Tabelle, um zu überprüfen, welche Funktionen des Schwachstellen- und Patch-Managements verfügbar sind.

Verfügbarkeit der Funktionen des Schwachstellen- und Patch-Managements

Funktion "Schwachstellen- und Patch-Management"	Testmodus	Kommerzieller Modus: Kaspersky Endpoint Security for Business Select	Kommerzieller Modus: Kaspersky Endpoint Security for Business Advanced, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Total Security for Business
Manuelles Beheben von Schwachstellen in der Software von Microsoft auf verwalteten Windows-Geräten Erstellen der Aufgabe *Schwachstellen schließen*	✓	✓	–
Manuelle Installation von Updates für die Software von Microsoft auf verwalteten Windows-Geräten Installation von Programm-Updates von Drittanbietern mittels der Aufgabe *Windows-Updates installieren*	–	✓	✓
Automatisches, regelbasiertes Installieren von Updates für Drittanbieter-Programme und Schließen von Schwachstellen in Drittanbieter-Programmen Erstellen der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* und Installation von Updates Hinzufügen einer Regel für die Installation von Updates	✓	–	✓

Über Anwendungen von Drittanbietern

Kaspersky Next Expert View kann Ihnen dabei helfen, auf Client-Geräten installierte Drittanbieter-Programme zu aktualisieren und die Schwachstellen in den Drittanbieter-Programmen zu beheben. Kaspersky Next Expert View kann Drittanbieter-Programme nur von der aktuellen installierten Version auf die neueste Version aktualisieren.

Die Liste mit Drittanbieter-Programmen kann geändert werden und wird dynamisch aktualisiert. Sie können überprüfen, ob Sie die Drittanbieter-Programme (die auf den Geräten der Benutzer installiert ist) mit Kaspersky Next Expert View aktualisieren können, indem Sie die Liste der verfügbaren Updates in der Kaspersky Next Expert View anzeigen.

Das im Folgenden beschriebene Verfahren dient ausschließlich dazu, die Liste der Drittanbieter-Programme anzuzeigen, die über Kaspersky Next Expert View 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 über Kaspersky Next Expert View aktualisieren können:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **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 **Anwendung** die Option **Kaspersky Next Expert View** 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.

Updates für Drittanbieter-Programme

Mit Kaspersky Next Expert View 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 Next Expert View sucht über die 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 Software von Drittanbietern, die auf den Geräten installiert ist, 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 Next Expert View Console wird mittels Deinstallation der vorherigen Programmversion und Installation der neuen Version durchgeführt.

Eine Benutzerinteraktion kann erforderlich sein, 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 im obigen Abschnitt genannten hinausgehen.

Aufgabe zur Installation von Updates für Drittanbieter-Programme

Wenn Metadaten von den Updates für Drittanbieter-Programme 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*

  Diese Aufgabe 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.

  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 Next Expert View, 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.

- Die Aufgabe *Windows-Updates installieren*

  Diese Aufgabe kann nur zur Installation von Windows-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, müssen Sie diese zur Liste der Updates in der vorhandenen Aufgabe hinzufügen oder eine Aufgabe des Typs *Windows-Updates installieren* erstellen.

Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

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.

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 Next Expert View 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:

   - Erstellen der Aufgabe Suche nach Schwachstellen und erforderlichen Updates
   - Einstellungen der Aufgabe zur 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 die Statistiken zur Update-Installation auf verwalteten Geräten anzeigen. Sie können beispielsweise die Anzahl der Geräte anzeigen, auf denen das ausgewählte Update nicht installiert ist, installiert wird oder auf denen die Update-Installation fehlgeschlagen ist.

   Anleitung: Anzeigen von Informationen über verfügbare Updates für Drittanbieter-Programme

3. **Konfigurieren der Installation von Updates**

   Wenn Kaspersky Next Expert View die Liste der Updates für Drittanbieter-Programme erhalten hat, können Sie diese mithilfe der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* oder *Windows-Updates 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.

   Die Aufgabe *Windows-Updates installieren* kann nur zur Installation von Windows-Updates verwendet werden.

   Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

Zum Installieren bestimmter Software-Updates müssen Sie die Endbenutzer-Lizenzvertrag (EULA) für die Installationssoftware akzeptieren. Wenn Sie die EULA ablehnen, wird das Software-Update nicht installiert.

Anleitung:

- Erstellen der Aufgabe Erforderliche Updates installieren und Schwachstellen schließen
- Erstellen der Aufgabe Windows-Updates installieren
- Anzeigen von Informationen zu verfügbaren Software-Updates von Drittanbietern

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. Die Standardhäufigkeit 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 *Windows-Updates 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 Beheben von Schwachstellen erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen ist.

   Anleitungen: Allgemeine Aufgabeneinstellungen

5. **Genehmigen und Ablehnen von Software-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. Wenn 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.

   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: Genehmigen und Ablehnen von Updates für Drittanbieter-Programme

6. **Ausführen einer Aufgabe zum Installieren von Updates**

   Starten Sie entweder die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Windows-Updates 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.

   Anleitung: Manuelles Starten einer Aufgabe

7. **Erstellen des Berichts zur Installation von Software-Updates von Drittanbietern (optional)**

   Um sicherzustellen, dass die Aufgabe erstellt und die Updates installiert werden, erstellen Sie den **Bericht über die Installationsergebnisse der Updates von Drittanbieterprogrammen** und zeigen Sie detaillierte Statistiken über die Installation der Updates in diesem Bericht.

   Anleitung: Bericht erstellen und anzeigen

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*

  Sie können die Aufgabe sowohl für die Installation von durch Microsoft bereitgestellte Updates von Windows Update, also auch für Software-Updates von anderen Hersteller verwenden.

- *Windows-Updates installieren*

  Sie können die Aufgabe nur zur Installation von Windows-Updates verwenden.

Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

Eine Benutzerinteraktion kann erforderlich sein, 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.

  Die Verfügbarkeit des Assistenten für die Installation von Updates hängt von dem Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab.

  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 Software-Updates von Drittanbietern 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 **Asset-Verwaltung → Assets (Geräte) → <Gerätename> → Erweitert → Verfügbare Updates**.
   - Um die Liste mit Updates für ein bestimmtes Programm zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge → Drittanbieteranwendungen → 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 Software-Update nicht installiert.

4. Wählen Sie eine der folgenden Varianten aus:

   - **Neue Aufgabe**

     Der Assistent für das Erstellen einer Aufgabe wird gestartet. Abhängig vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ist entweder die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder 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 wollen. Wählen Sie entweder eine Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* oder eine Aufgabe des Typs *Windows-Updates installieren*. Wenn Sie eine Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* auswählen, wird der ausgewählten Aufgabe automatisch eine neue Regel für die Installation der gewählten Updates hinzugefügt. Wenn Sie eine Aufgabe des Typs *Windows-Updates installieren* auswählen, werden die ausgewählten Updates 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 **Asset-Verwaltung → 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 Software-Updates von Drittanbietern mithilfe des Assistenten für die Installation von Updates

Die Verfügbarkeit dieser Funktion hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab.

Um eine Aufgabe zur Installation der Software-Updates von Drittanbietern mithilfe des Assistenten für die Installation von Updates zu installieren, gehen Sie wie folgt vor:

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** zeigt Ihnen 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** (nur für Updates von Windows Update verfügbar)

  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** (nur für Updates von Drittanbieter-Programmen verfügbar)

  Diese Option ist nur für Updates von Dritthersteller-Anwendungen verfügbar. Kaspersky Next Expert View 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 Anwendungs-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** (nur für Updates von Windows Update verfügbar)

  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** (nur für Updates von Drittanbieter-Programmen verfügbar)

  Diese Option ist nur für Updates von Dritthersteller-Anwendungen verfügbar. Kaspersky Next Expert View 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 Anwendungs-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 für die Installation von Updates hinzugefügt haben, wird im Assistenten für das Erstellen einer Aufgabe angezeigt. Wenn Sie den Assistenten für das Erstellen einer Aufgabe 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 Next Expert View eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Drittanbieter-Programme, die auf den verwalteten Geräten installiert sind.

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 **Asset-Verwaltung** → **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 Next Expert View 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 **Anwendungseinstellungen** die folgenden Einstellungen an:

    - **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

      Wenn Kaspersky Next Expert View 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:

      - Administrationsserver für Kaspersky Next Expert View (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.

- Wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** gesetzt ist, fragt Kaspersky Next Expert View unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) keine Informationen über Updates ab.

- **Nach Schwachstellen und Updates von Drittanbietern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Next Expert View 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 Anwendungen 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 Next Expert View 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 Next Expert View 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 Apps installiert sind. Diese Liste ist standardmäßig leer.

- **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 Next Expert View 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 der Einstellung im Tool Remote-Diagnose für Kaspersky Next Expert View 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 Next Expert View 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:

  - Administrationsserver für Kaspersky Next Expert View (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.

- Wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** gesetzt ist, fragt Kaspersky Next Expert View unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) keine Informationen über Updates ab.

- **Nach Schwachstellen und Updates von Drittanbietern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Next Expert View 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 Anwendungen 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 Next Expert View 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 Next Expert View 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 Apps installiert sind. Diese Liste ist standardmäßig leer.

- **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 Next Expert View 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 der Einstellung im Tool Remote-Diagnose für Kaspersky Next Expert View 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 Verfügbarkeit der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Software von Drittanbietern, 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 zur Installation von Updates einer bestehenden Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* hinzu.

Die Aufgaben zur Installation von Programm-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

So erstellen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **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 Next Expert View den Aufgabentyp **Erforderliche Updates installieren und 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. 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 Anwendungsversion 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 Next Expert View 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 der Einstellung im Tool Remote-Diagnose für Kaspersky Next Expert View 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 für das Betriebssystem 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 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.

- **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.

- **Erzwungenes Schließen von Anwendungen in gesperrten Sitzungen nach (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 auf der Seite **Erstellung der Aufgabe abschließen** die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die standardmäßigen Aufgabeneinstellungen ändern. 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

Die Verfügbarkeit dieser Funktion hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab.

Bei der Installation von Software-Updates oder dem Schließen von Schwachstellen in Programmen mithilfe 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 Anwendungs-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 Client-Geräten bereitgestellt werden.

Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

Um die Aufgabe "Windows-Updates installieren" zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **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 Next Expert View 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 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.

- **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 zum Status von Update-Installationen**.

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 **Asset-Verwaltung → Assets (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.

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** → **Drittanbieteranwendungen** → **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 Next Expert View 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 Next Expert View 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.

Suchen und Schließen von Software-Schwachstellen

Kaspersky Next Expert View 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 Next Expert View verwendet Merkmale aus der Datenbank mit bekannten Schwachstellen, und die Windows Update-Datenbank, um Schwachstellen in Programmen zu finden. Die Datenbank mit bekannten Schwachstellen wird von Kaspersky-Spezialisten erstellt und verwaltet. 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 Next Expert View verwendet zur Suche nach Schwachstellen in Programmen die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*.

Beheben von Schwachstellen in Programmen

Zum Beheben von Schwachstellen in Programmen verwendet Kaspersky Next Expert View die Programm-Updates der Software-Hersteller. Sie können jederzeit die Liste mit den Schwachstellen in Programmen anzeigen. Die Metadaten der Programm-Updates werden im Rahmen der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* automatische in die Datenverwaltung des Administrationsservers und in die Datenverwaltungen der Verteilungspunkte heruntergeladen. Sie können diese Aufgabe mit dem Schnellstartassistenten von Kaspersky Next Expert View oder manuell erstellen.

Software-Updates zur Behebung von Schwachstellen können in Form von vollständigen Programmpaketen oder Patches bereitgestellt werden. Software-Updates, die Schwachstellen in Programmen beheben, werden als *Korrekturen* bezeichnet. In Kaspersky Next Expert View werden Schwachstellen mithilfe *empfohlener Korrekturen* geschlossen. Empfohlene Korrekturen sind Programm-Updates, deren Installation von den Kaspersky-Experten empfohlen wird.

Abhängig vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz können Sie entweder die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Schwachstellen schließen* verwenden, um Schwachstellen in Programmen zu beheben.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* behebt automatisch mehrere Schwachstellen durch die Installation empfohlener Korrekturen. Für diese Aufgabe können Sie bestimmte Regeln manuell konfigurieren, um mehrere Schwachstellen zu beheben.

Mithilfe der Aufgabe *Schwachstellen schließen* können Sie Schwachstellen durch die Installation empfohlener Korrekturen für Software von Microsoft schließen.

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.

Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

Eine Benutzerinteraktion kann erforderlich sein, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, die Drittanbieter-Anwendung zu schließen, wenn es gerade geöffnet ist.

Zum Schließen bestimmter Schwachstellen in Programmen müssen Sie den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren, wenn dies angefordert wird. Wenn Sie die EULA ablehnen, kann die Schwachstelle im Programm nicht geschlossen werden.

Die Informationen zu jeder geschlossenen Schwachstelle werden für 90 Tage auf dem Administrationsserver gespeichert. Danach werden Sie automatisch gelöscht.

Beheben von Schwachstellen in Programmen

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 in Programmen im Betriebssystem und in Software von Drittanbietern, einschließlich Microsoft-Software, ist mithilfe der Aufgabe *Schwachstellen schließen* oder der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* möglich.

Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

Eine Benutzerinteraktion kann erforderlich sein, 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.

Die Verfügbarkeit dieser Funktion hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab.

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 **Asset-Verwaltung → Assets (Geräte) → <Gerätename> → Erweitert → Schwachstellen in Programmen**.
   - Um die Schwachstellenliste für ein bestimmtes Programm zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge → Drittanbieteranwendungen → 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 Schwachstellen in Programmen müssen Sie den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren, wenn dies angefordert wird. 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. Abhängig vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz wird entweder die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder 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. Wählen Sie abhängig vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz entweder eine Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* oder eine Aufgabe des Typs *Schwachstellen schließen* aus. Wenn Sie eine Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* auswählen, wird eine neue Regel zum Schließen der ausgewählten Schwachstellen der ausgewählten Aufgabe automatisch hinzugefügt. Wenn Sie eine Aufgabe des Typs *Schwachstellen schließen* auswählen, werden die ausgewählten Schwachstellen 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 **Asset-Verwaltung → 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 für das Schließen von Schwachstellen

Die Verfügbarkeit des Assistenten für das Schließen von Schwachstellen ist davon abhängig, welche Lizenz Sie verwenden und in welchem Modus Kaspersky Next Expert View ausgeführt wird.

Um Schwachstellen in Programmen mithilfe des Assistenten für das Schließen von Schwachstellen zu beheben, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Patch-Management → Schwachstellen in Programmen**.

   Eine Seite mit der Liste von Schwachstellen in Programmen von Drittanbietern, 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 Anwendungen des ausgewählten Anbieters** (nur für Schwachstellen in Drittanbieter-Programmen verfügbar)

  - **Regel zum Schließen von Schwachstellen in allen Versionen der ausgewählten Anwendung** (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 Typs** (nur für Schwachstellen in der Software von Microsoft verfügbar)
- **Regel zum Schließen von Schwachstellen in Anwendungen des ausgewählten Anbieters** (nur für Schwachstellen in Drittanbieter-Programmen verfügbar)
- **Regel zum Schließen von Schwachstellen in allen Versionen der ausgewählten Anwendung** (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 für das Erstellen einer Aufgabe 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 Software von Microsoft, die sich auf verwalteten Windows-Geräten befinden.

Die Verfügbarkeit dieser Funktion hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab. 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.

Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

Eine Benutzerinteraktion kann erforderlich sein, 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 **Asset-Verwaltung** → **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 Next Expert View 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**.
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 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.

- **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 auf der Seite **Erstellung der Aufgabe abschließen** die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die standardmäßigen Aufgabeneinstellungen ändern. 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 Verfügbarkeit der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Software von Drittanbietern, 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 zur Installation von Updates einer bestehenden Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* hinzu.

Die Aufgaben zur Installation von Programm-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Next Expert View verwenden, und von dem Modus, in dem Kaspersky Next Expert View arbeitet.

So erstellen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **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 Next Expert View den Aufgabentyp **Erforderliche Updates installieren und 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. 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 Anwendungsversion 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 Next Expert View 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 der Einstellung im Tool Remote-Diagnose für Kaspersky Next Expert View 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 für das Betriebssystem 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 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.

- **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.

- **Erzwungenes Schließen von Anwendungen in gesperrten Sitzungen nach (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 auf der Seite **Erstellung der Aufgabe abschließen** die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die standardmäßigen Aufgabeneinstellungen ändern. 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

Die Verfügbarkeit dieser Funktion hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab.

Bei der Installation von Software-Updates oder dem Schließen von Schwachstellen in Programmen mithilfe 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 Anwendungs-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.

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 **Asset-Verwaltung** → **Assets (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 **Asset-Verwaltung → Assets (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.

Szenario: Suchen und Schließen von Schwachstellen in Programmen

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 Cloud Console wurde in Ihrem Unternehmen bereitgestellt.
- Sie haben in Ihrer Organisation verwaltete Geräte, auf denen Windows ausgeführt wird.

Schritte

Das Erkennen und Schließen von Schwachstellen in Programmen erfolgt schrittweise:

1. **Scannen nach Schwachstellen in den auf den Client-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 Next Expert View 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 von Kaspersky Next Expert View erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, starten Sie ihn jetzt oder erstellen Sie die Aufgabe manuell.

   Anleitung: Die Aufgabe Suche nach Schwachstellen und erforderlichen Updates erstellen

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:

   - Informationen über Schwachstellen in Programmen anzeigen
   - Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten

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 Software von Drittanbietern, 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. Die Verfügbarkeit dieser Aufgabe hängt vom Modus der Kaspersky Next Expert View und Ihrer aktuellen Lizenz ab. Um Schwachstellen in Programmen zu beheben, verwendet die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die empfohlenen Software-Updates.

Die Aufgabe *Schwachstellen schließen* verwendet empfohlene Korrekturen für Software von Microsoft.

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: Beheben von Schwachstellen in Drittanbieter-Programmen, Erstellen der Aufgabe Erforderliche Updates installieren und Schwachstellen schließen

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 Korrekturen für Software von Microsoft auswählen 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: Ignorieren von Schwachstellen in Programmen

6. **Aufgabe zum Schließen von Schwachstellen ausführen**

   Starten Sie entweder die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Schwachstellen 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-Software, einschließlich Microsoft-Software, suchen und solche Schwachstellen beheben können.

   Anleitung: Bericht erstellen und anzeigen

8. **Überprüfen der Konfiguration zum Finden und Schließen von Schwachstellen in Programmen von Drittanbietern**

   Stellen Sie folgende Punkte sicher:

   - Die Liste der Schwachstellen in Programmen auf den verwalteten Geräten ist nicht leer.
   - In der Aufgabenliste existiert eine Aufgabe zum Schließen von Schwachstellen.

- Die Aufgaben zur Suche und zum Beheben von Schwachstellen in Programmen sind so geplant, dass sie nacheinander gestartet werden. Prüfen Sie die Eigenschaften dieser Aufgaben und vergleichen Sie die Aufgabenzeitpläne.

- Die Aufgabe zum Beheben von Schwachstellen in Programmen wurde erfolgreich abgeschlossen. Prüfen Sie die Informationen auf der Registerkarte **Ergebnisse** im Eigenschaftenfenster der Aufgabe.

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 Software-Updates mit den Regeln abgeglichen, die in den Aufgabeneinstellungen angegeben sind. Alle Programm-Updates, ausgenommen Windows-Updates, welche die Kriterien der Regeln erfüllen, werden in die Datenverwaltungen der Verteilungspunkte heruntergeladen und installiert, um die Schwachstellen in Programmen zu beheben. Um Windows-Updates zu installieren, müssen Sie auf Ihren verwalteten Geräten den Zugriff auf die öffentlichen Server von Microsoft Update gewährleisten.

Wenn Sie die Aufgabe *Schwachstellen schließen* erstellt haben, werden nur Schwachstellen in Programmen von Microsoft behoben.

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 im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Ereignis-Datenverwaltung**.

3. Geben Sie für Informationen über behobene Schwachstellen die maximale Speicherdauer in der Datenbank an.

   Standardmäßig beträgt die Speicherdauer 7 Tage im Testmodus und 60 Tage im kommerziellen Modus. Das maximale Limit beträgt 14 Tage im Testmodus und 365 Tage im kommerziellen Modus.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die maximale Speicherdauer für Informationen über behobene Schwachstellen wird auf die angegebene Anzahl von Tagen begrenzt.

Verwalten des Programmstarts auf Client-Geräten

In diesem Abschnitt werden die Funktionen von Kaspersky Next Expert View 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 Komponente "Programmkontrolle" beginnend mit Kaspersky Endpoint Security 11.2 für Linux verfügbar.

Erforderliche Vorrausetzungen

- Kaspersky Next Expert View wurde in Ihrem Unternehmen bereitgestellt.
- Die Richtlinie von Kaspersky Endpoint 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: Liste der auf Client-Geräten installierten ausführbaren Dateien abrufen und anzeigen

2. **Erstellen von Kategorien für die 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: Manuell zu erweiternde Programmkategorie erstellen, Programmkategorie mit ausführbaren Dateien aus ausgewählten Geräten erstellen

3. **Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows**

   Konfigurieren Sie die Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows anhand der Kategorien, die Sie beim vorherigen Schritt erstellt haben.

   Anleitung: Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows

4. **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. Wenn das Testen aktiviert ist, blockiert Kaspersky Endpoint Security für Windows keine ausführbaren Dateien, deren Start durch die Regeln der Programmkontrolle unzulässig ist, sondern sendet Benachrichtigungen über deren Start an den Administrationsserver.

   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: Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows konfigurieren Folgen Sie dieser Anweisung und aktivieren Sie beim Konfigurieren den Testbetrieb.

5. **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 Programmkategorie manuell ausführbare Dateien hinzufügen, die sich auf Ereignisse der Programmkontrolle beziehen.

   Anleitung: Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

6. **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: Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows konfigurieren Folgen Sie dieser Anweisung und deaktivieren Sie beim Konfigurieren den Testbetrieb.

7. **Überprüfen der Konfiguration der Programmkontrolle**

   Stellen Sie folgende Punkte sicher:

   - Die Liste der Kategorien für ausführbare Dateien ist nicht leer. Prüfen Sie die Liste der Kategorien und stellen Sie sicher, dass sie die Kategorien enthält, die Sie angepasst haben.
   - Zur Konfiguration der Programmkontrolle wurden erstellte Kategorien für ausführbare Dateien verwendet. Prüfen Sie die Einstellungen der Richtlinie für Kaspersky Endpoint Security für Windows und stellen Sie sicher, dass Sie "Programmkontrolle" unter **Programmeinstellungen** → **Sicherheitskontrolle** → **Programmkontrolle** angepasst haben.
   - Die Regeln der "Programmkontrolle" werden im Betriebsmodus angewendet. Prüfen Sie den Modus in der Richtlinie für Kaspersky Endpoint Security für Windows und stellen Sie sicher, dass Sie den **Testmodus** unter **Programmeinstellungen** → **Sicherheitskontrolle** → **Programmkontrolle** deaktiviert haben.

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

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 verfügbar für Kaspersky Endpoint Security für Windows und für Kaspersky Endpoint Security für Linux (ab Version 11.2). Alle Anleitungen in diesem Abschnitt beschreiben die Konfiguration der "Programmkontrolle" für Kaspersky Endpoint Security.

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. Der Modus *Deny-Liste* 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 Next Expert View existieren zwei 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.

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

Aufrufen und Anzeigen einer Liste der auf Client-Geräten installierten Programme

Kaspersky Next Expert View 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.

Um die Liste mit auf verwalteten Geräten installierten Anwendungen anzuzeigen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **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 **Tabelleneinstellungen** 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 **Asset-Verwaltung** → **Assets (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

Abrufen und Anzeigen einer Liste der auf Client-Geräten installierten ausführbaren Dateien

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)

Sie können die Auslastung der Datenbank verringern und gleichzeitig Informationen über die installierten Anwendungen erhalten. Dazu empfehlen wir, dass Sie eine Bestandsaufnahme auf den Referenzgeräten durchführen, auf denen ein Standardpaket von Software installiert ist. Die empfohlene Anzahl an Geräten beträgt 1-3.

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → 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 **Anwendung** 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 konfiguriert. 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

Nach Ausführung der Aufgabe **Inventarisierung** wird die Liste der auf verwalteten Geräten installierten 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.

So zeigen Sie sich die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien auf an:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Ausführbare Dateien**.

Auf der Seite wird die Liste der auf Client-Geräten installierten ausführbaren Dateien angezeigt.

Bei Bedarf können Sie die ausführbare Datei des verwalteten Geräts an das Gerät senden, auf dem Ihre Kaspersky Next Expert View geöffnet ist.

So senden Sie eine ausführbare Datei:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **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.

   Bevor Sie die ausführbare Datei senden, stellen Sie sicher, dass das verwaltete Gerät eine direkte Verbindung zum Administrationsserver besitzt. Um dies zu tun, können Sie entweder einen Verteilungspunkt als Push-Server mit Standardport (13295) verwenden oder das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** aktivieren. Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

4. Klicken Sie auf die Schaltfläche **Senden**.

Die ausgewählte ausführbare Datei wird heruntergeladen, um sie anschließend an das Gerät mit Ihrer geöffneten Kaspersky Next Expert View 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** → **Drittanbieteranwendungen** → **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. Gehen Sie im Schritt **Bedingungskriterien** wie folgt vor:

   a. Wählen Sie einen Regeltyp für die Erstellung einer Kategorie von 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.

     > Informationen über Zertifikate können nur aus ausführbaren Dateien im PE-Format (.exe, .dll, .sys) extrahiert werden.

   - **Pfad der Anwendung 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.

    Datei-Hash

    Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Next Expert View 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 Next Expert View 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.

b. Fügen Sie bei Bedarf einen Kommentar in das Feld **Beschreibung** ein. Sie können maximal 1000 Zeichen eingeben.

Sie können den Kommentar später ändern oder löschen, indem Sie in den Eigenschaften der Programmkategorie auf die Registerkarte **Bedingungen** klicken und anschließend in der Spalte **Kriterium der Bedingung** den Link mit der Bedingung anklicken, für welche Sie den Kommentar ändern oder löschen möchten.

> Wenn Sie den Regeltyp **Aus der KL-Kategorie** auswählen, können Sie einen Kommentar für alle Bedingungen hinzufügen, die basierend auf diesem Regeltyp erstellt werden sollen. Sie können den Kommentar für jede Bedingung separat bearbeiten oder löschen.

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.

   Bei Bedarf können Sie in dem Feld **Beschreibung** einen Kommentar hinzufügen. Sie können maximal 1000 Zeichen eingeben.

   Sie können den Kommentar später ändern oder löschen, indem Sie in den Eigenschaften der Programmkategorie auf die Registerkarte **Ausschlüsse** klicken und anschließend in der Spalte **Kriterium der Bedingung** den Link mit der Bedingung anklicken, für welche Sie den Kommentar ändern oder löschen möchten.

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

Erstellen einer Programmkategorie mit ausführbaren Dateien aus ausgewählten Geräten

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.

Um eine Kategorie zu erstellen, die ausführbare Dateien von ausgewählten Geräten enthält, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programmkategorien**.

   Die Seite mit der Liste der Kategorien für ausführbare Dateien 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 Next Expert View 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 Next Expert View 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.

Liste der Programmkategorien anzeigen

Sie können die Liste der angepassten Programmkategorien und die Einstellungen der einzelnen Programmkategorien anzeigen.

Um die Liste der Programmkategorien anzuzeigen,

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programmkategorien**.

Die Seite mit einer Liste der Programmkategorien wird angezeigt.

Um die Eigenschaften einer Programmkategorie anzuzeigen,

Klicken Sie auf den Namen der Programmkategorie.

Das Eigenschaftenfenster der Programmkategorie wird angezeigt. Die Eigenschaften sind auf mehreren Registerkarten angeordnet.

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 **Asset-Verwaltung** → **Richtlinien**.

   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 **Anwendungseinstellungen → Sicherheitskontrollen → Programmkontrolle**.

   Das Fenster **Programmkontrolle** mit den entsprechenden Eigenschaften wird angezeigt.

4. Die Option **Programmkontrolle** ist standardmäßig aktiviert. Setzen Sie den Umschalter auf **Programmkontrolle DEAKTIVIERT**, um die Option zu deaktivieren.

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 den Computer nach Auswahl der Option **Laden von DDL-Modulen überwachen** neu, wenn Kaspersky Endpoint Security für Windows alle DLL-Module und -Treiber überwachen soll, einschließlich jener, 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

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 → 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 Datei, die das Ereignis auslöste** 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:

     - **Zertifikatinformationen (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.

     - **Zertifikatinformationen (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 zu den Regeln der Kategorie hinzufügen möchten

- **Nur MD5 (Modus eingestellt. Nur für 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

Erstellen eines Installationspakets eines Drittanbieterprogramms aus der Kaspersky-Datenbank

Mit Kaspersky Security Center Web Console können Sie Installationspakete erstellen, um eine Remote-Installation von Drittanbieter-Anwendungen durchzuführen. Solche Drittanbieterprogramme sind in einer dedizierten Kaspersky-Datenbank enthalten.

Das Erstellen von Installationspaketen für Drittanbieter-Programme aus der Kaspersky-Datenbank steht nur unter der Lizenz für das Schwachstellen- und Patch-Management zur Verfügung.

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 eine ausgewählte Anwendung 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
  - **Anwendung**

    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.

- **Anwendungsversion**

  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.

- **Anwendungsfamilie**

  Gibt den Namen der Programmfamilie an, zu welcher dieses Update gehört.

- **Anwendung**

  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 Next Expert View können Sie den Anwendungen in der Programm-Registry Tags hinzufügen. Ein Tag ist eine Bezeichnung, anhand derer Programme 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** → **Drittanbieteranwendungen** → **Anwendungs-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** → **Drittanbieteranwendungen** → **Anwendungs-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** → **Drittanbieteranwendungen** → **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** → **Drittanbieteranwendungen** → **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** → **Drittanbieteranwendungen** → **Anwendungs-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.

Konfigurieren des Administrationsservers

Dieser Abschnitt beschreibt den Konfigurationsprozess und die Eigenschaften des Kaspersky Security Center Administrationsservers.

Hierarchie des Administrationsservers

Einige Kundenunternehmen wie MSPs betreiben möglicherweise mehrere Administrationsserver. Die Verwaltung mehrerer vereinzelter Administrationsserver ist unpraktisch, deshalb es ist zweckmäßig, sie in einer Hierarchie zusammenzufassen. Für den Administrationsserver in der Kaspersky Infrastruktur sind jeweils sowohl der primären Administrationsserver als auch der sekundäre Administrationsserver in Ihrem Netzwerk sekundäre Server. Sie können sowohl einen Windows-basierten als auch einen Linux-basierten Administrationsserver hinzufügen.

Eine "Primär/Sekundär"-Konfiguration für zwei Administrationsserver bietet die folgenden Möglichkeiten:

- Der sekundäre Administrationsserver erbt vom primären Administrationsserver die Richtlinien Aufgaben, Benutzerrollen und Installationspakete, 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.
- Als Update-Quelle für einen sekundären Administrationsserver kann ein primärer Administrationsserver verwendet werden.

Die Hierarchie der Administrationsserver unterstützt den Mandantenfähigkeitsmodus. Dieser Modus ermöglicht es einem Hauptadministrator, mehrere Clients unabhängig voneinander zentral zu verwalten. Jedes Kundenunternehmen oder Büro ist von anderen isoliert und wird als Mandant bezeichnet. Sie können einem Mandanten mehrere verwaltete Geräte mit den dazugehörigen Daten, Einstellungen, Richtlinien und Aufgaben zuweisen und die Benutzerrechte nach Mandanten konfigurieren.

Ein primärer Administrationsserver, der in der Hauptinfrastruktur des Unternehmens installiert ist, fungiert als primärer Mandant. Der primäre Administrationsserver ermöglicht es sekundären oder virtuellen Administrationsservern – seinen isolierten Mandanten –, selbstständig ihre eigenen Ereignisse zu empfangen und zu verarbeiten und mit ihren eigenen Ressourcen, Diensten und Konfigurationen zu arbeiten.

Ein Dienstanbieter mit mehreren Kundenunternehmen kann die Funktionen von Kaspersky Next Expert View, einschließlich der Aggregation von Alarmen und Reaktionsmaßnahmen, für jedes Kundenunternehmen unabhängig voneinander bereitstellen. Zu diesem Zweck verbindet der Dienstanbieter sekundäre oder virtuelle Administrationsserver als Mandanten für jedes Kundenunternehmen. Der Dienstanbieter stellt Dienste unter Verwendung seines eigenen Personals und seiner eigenen Ressourcen bereit.

Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen

Sie können einen lokal ausgeführten Administrationsserver zum sekundären Administrationsserver ernennen und so eine Hierarchie vom Typ "primär/sekundär" festlegen. Für den Administrationsserver in der Kaspersky Infrastruktur sind jeweils sowohl der primären Administrationsserver als auch der sekundäre Administrationsserver in Ihrem Netzwerk sekundäre Server. Sie können sowohl einen Windows-basierten als auch einen Linux-basierten Administrationsserver hinzufügen.

Um einen Administrationsserver, der zum Verbinden verfügbar ist, als sekundären Server hinzuzufügen:

1. Stellen Sie sicher, dass auf dem vorgesehenen sekundären Administrationsserver die Kaspersky Security Center Web Console installiert ist.

2. Laden Sie auf dem vorgesehenen sekundären Administrationsserver das Zertifikat des Administrationsservers herunter und speichern Sie es so, dass Sie es dem primären Administrationsserver während der Schritte des Assistenten für das Hinzufügen eines sekundären Administrationsservers hinzufügen können.

3. Führen Sie die folgenden Schritte in der Kaspersky Security Center Web Console auf dem zukünftigen sekundären Administrationsserver aus (Alternativ können Sie den Administrator des zukünftigen sekundären Administrationsservers dazu auffordern, diese Schritte auszuführen):

   a. Wechseln Sie zu den Eigenschaften des zukünftigen primären Administrationsservers, indem Sie im Hauptmenü auf den Namen des Administrationsservers klicken.

      Alternativ dazu können Sie die Eigenschaften des erforderlichen Administrationsservers über den Navigationsbereich aufrufen. Wählen Sie dazu im Hauptmenü einen beliebigen Abschnitt (außer **Marketplace**, **Konsolen-Navigation** und **Einstellungen**) und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen des gewünschten Administrationsservers und klicken Sie anschließend auf das Einstellungssymbol (⚙).

   b. Wechseln Sie im neuen Eigenschaftsfenster auf der Registerkarte **Allgemein** zum Abschnitt **Hierarchie der Administrationsserver**.

   c. Aktivieren Sie die Option **Dieser Administrationsserver ist in der Server-Hierarchie sekundär**.

   d. Wählen Sie für den Typ des primären Administrationsservers die Option **Cloud Console** aus.

      Die Felder für die Konfiguration der Verbindungseinstellungen zwischen sekundären und primären Administrationsserver werden verfügbar.

   e. Geben Sie in den Feldern **Adresse des HDS-Servers (des primären Administrationsservers in Cloud Console)** und **Ports des HDS-Servers** die Adresse und den Port des primären Administrationsservers mit Kaspersky Next Expert View an.

      Die HDS-Serveradresse und HDS-Serverports finden Sie auf dem Kaspersky Next Expert View Administrationsserver im Abschnitt **Hierarchie der Administrationsserver** auf der Registerkarte **Allgemein** des Eigenschaftenfensters. Sie können diese Informationen kopieren und anschließend in den Feldern des sekundären Administrationsservers einfügen.

f. Klicken Sie auf die Schaltfläche **Zertifikat des primären Administrationsservers angeben** und wählen Sie anschließend das Zertifikat aus.

Herunterladen können Sie das Zertifikat von dem Kaspersky Next Expert View Administrationsserver durch Klicken auf die Schaltfläche **Zertifikat des Administrationsservers anzeigen** im Abschnitt **Hierarchie der Administrationsserver** auf der Registerkarte **Allgemein** des Eigenschaftenfensters.

g. Klicken Sie auf die Schaltfläche **Zertifikate des Hosted Discovery Service angeben** und wählen Sie anschließend das Zertifikat aus.

Herunterladen können Sie das Zertifikat von dem Kaspersky Next Expert View Administrationsserver durch Klicken auf die Schaltfläche **HDS Root CA Zertifikat** im Abschnitt **Hierarchie der Administrationsserver** auf der Registerkarte **Allgemein** des Eigenschaftenfensters.

h. Wenn Sie einen Proxyserver für die Verbindung mit dem Kaspersky Next Expert View Administrationsserver (d.h. mit dem primären Server in der von Ihnen angelegten Hierarchie) verwenden, geben Sie dies und die Anmeldeinformationen des Proxyservers an.

i. Wählen Sie die Option **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**, wenn sich der sekundäre Administrationsserver in einer demilitarisierten Zone befindet.

j. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und das Fenster zu verlassen.

4. Klicken Sie im Hauptmenü von Kaspersky Next Expert View auf den Namen des Administrationsservers.

5. Wechseln Sie auf der folgenden Eigenschaftenseite auf die Registerkarte **Administrationsserver**.

6. Wählen Sie das Kontrollkästchen neben der Administrationsgruppe aus, zu der Sie den virtuellen sekundären Administrationsserver hinzufügen möchten.

7. 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.

8. Füllen Sie die folgenden Felder aus:

- **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.

9. Wenn Sie einen Proxyserver für die Verbindung mit dem Kaspersky Next Expert View Administrationsserver (d.h. mit dem zukünftigen primären Server) verwenden, geben Sie dies und die Anmeldeinformationen des Proxyservers an.

10. Folgen Sie den weiteren Schritten des Assistenten.

Nach Abschluss des Assistenten wird eine "primärer/sekundär"-Hierarchie 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.

Speicherdauer von Ereignissen für die gelöschten Geräte konfigurieren

In Kaspersky Next Expert View werden Ereignisse in einer Ereignis-Datenverwaltung gespeichert. Sie können nicht angeben, wie viele Ereignisse in der Ereignis-Datenverwaltung gespeichert werden sollen.

Im Abschnitt **Ereignis-Datenverwaltung** des Fensters der Eigenschaften des Administrationsservers können Sie die maximale Speicherdauer von Ereignissen für die gelöschten Geräte konfigurieren. Standardmäßig beträgt die Speicherdauer 1000 Tage.

So konfigurieren Sie die Anzahl der Tage, für die Ereignisse mit Bezug auf gelöschte Geräte gespeichert werden:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Ereignis-Datenverwaltung** aus.

3. Aktivieren Sie die Option **Ereignisse von gelöschten Geräten weiterhin speichern**.

4. Geben Sie im Bearbeitungsfeld **Maximale Speicherdauer (Tage)** die Anzahl der Tage an, für die Ereignisse mit Bezug auf gelöschte Geräte gespeichert werden sollen.

   Die Anzahl der Tage, an denen Ereignisse zu den gelöschten Geräten gespeichert werden, ist durch den angegebenen Wert begrenzt.

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.

E-Mails zu Ereignissen zusammenfassen

Während des Vorgangs generieren Kaspersky Next Expert View und verwaltete Kaspersky-Anwendungen Ereignisse. Jedes Ereignis gehört einem bestimmten Typ und einer Signifikanz (*Kritisch*, *Funktionsfehler*, *Warnung*, *Infomeldung*) an. Abhängig von den Umständen, unter denen das Ereignis aufgetreten ist, kann Kaspersky Next Expert View demselben Ereignistyp unterschiedliche Signifikanzen zuweisen.

Kaspersky Next Expert View versendet automatisch Benachrichtigungen über Ereignisse per E-Mail. Kaspersky Next Expert View versendet Benachrichtigungen über Ereignisse, die im Fenster **Eigenschaften des Administrationsservers** auf der Registerkarte **Konfiguration von Ereignissen** aufgeführt werden. Gemeinsame Benachrichtigungseinstellungen werden für alle Ereignistypen verwendet.

Um die Anzahl der zu sendenden E-Mails einzuschränken, fasst Kaspersky Next Expert View in bestimmten Zeiträumen Ereignisse mit derselben Signifikanz zusammen. Die Werte der Zeiträume werden von Kaspersky-Spezialisten verwaltet. Bei Bedarf können Sie Informationen über die Zeiträume für das Zusammenfassen anzeigen, indem Sie auf **diesen Link** klicken.

Nach dem Senden einer Benachrichtigung über ein neues Ereignis mit einer bestimmten Signifikanz führt der Administrationsserver die folgenden Aktionen aus:

1. Er aktiviert einen 15-minütigen Zähler

2. Nach 15 Minuten:

   - Wenn keine Ereignisse mit gleicher oder niedrigerer Signifikanz aufgetreten sind, wird der Zähler zurückgesetzt.

   - Wenn mindestens ein Ereignis mit gleicher oder niedrigerer Signifikanz auftritt, sendet er eine zusammengefasste E-Mail mit Informationen zu den Ereignissen an die Empfänger und aktiviert anschließend einen weiteren Zähler mit einem dreistündigen Intervall.

     In diesem Fall führt der Administrationsserver eine der folgenden Aktionen aus:

     - Wenn während dieser drei Stunden keine Ereignisse mit der relevanten (oder einer niedrigeren) Signifikanz aufgetreten sind, werden beide Zähler zurückgesetzt.

     - Wenn mindestens ein Ereignis mit gleicher oder niedrigerer Signifikanz auftritt, sendet er eine zusammengefasste E-Mail mit Informationen zu den Ereignissen an die Empfänger und aktiviert den Zähler mit dem dreistündigen Intervall anschließend erneut.

Wenn innerhalb der beiden Intervalle (15 Minuten oder 3 Stunden) mindestens ein Ereignis mit einer höheren Signifikanz auftritt, führt der Administrationsserver nacheinander die folgenden Aktionen aus:

a. Er sendet eine zusammenfassende E-Mail mit Informationen über zuvor aufgetretene Ereignisse an die Empfänger, ohne bis zum Ende des Intervalls zu warten.

b. Er sendet den Empfängern eine E-Mail über das neue Ereignis mit der höheren Signifikanz.

c. Er setzt die aktivierten Zähler zurück.

d. Er aktiviert einen neuen 15-minütigen Zähler und das hier beschriebene Szenario wird erneut gestartet.

Infolgedessen erhalten Empfänger zusammengefasste E-Mail-Nachrichten gemäß folgender Vorlage: "<Anzahl> <Signifikanz> (einschließlich niedrigerer Signifikanzen) Ereignisse sind aufgetreten".

Wenn Sie sofort Benachrichtigungen von Benutzern erhalten möchten, können Sie die Integration zwischen Kaspersky Next Expert View und SIEM konfigurieren und anschließend die Benachrichtigungen über die erforderlichen Ereignisse von SIEM anpassen.

Einschränkungen bei der Verwaltung von sekundären Administrationsservern, die lokal über Kaspersky Next Expert View ausgeführt werden

Nachdem Sie mithilfe der entsprechenden Option in Kaspersky Next Expert View zu einem lokal ausgeführten sekundären Administrationsserver gewechselt sind, erlegt das Programm der Verwaltung dieses sekundären Administrationsservers bestimmte Einschränkungen auf. Die folgenden Einstellungen für die Verwendung von Kaspersky Next Expert View sind für den Benutzer nicht mehr verfügbar:

- In den Richtlinieneinstellungen von Administrationsagent und Administrationsserver sind die Registerkaten **Konfiguration von Ereignissen** und **Anwendungseinstellungen** nicht verfügbar. Es können keine neuen Richtlinien erstellt werden.
- In den Aufgabeneinstellungen von Administrationsagent und Administrationsserver sind die Registerkarten **Konfiguration von Ereignissen** und **Anwendungseinstellungen** nicht verfügbar. Es können keine neuen Aufgaben erstellt werden.
- Die Verwaltung des Administrationsagenten und des Administrationsservers ist ebenso wie das Eigenschaftenfenster des sekundären Administrationsservers nicht verfügbar.
- Der Schnellstartassistent ist nicht verfügbar.
- Die Speicher- und Benachrichtigungseinstellungen für Ereignisse des Administrationsagenten und des Administrationsservers können nicht geändert werden.
- Der Abschnitt **Aktuelle Anwendungsversionen** ist nicht verfügbar.
- Der Abschnitt **Installationspakete** ist nicht verfügbar.

Liste mit sekundären Administrationsservern anzeigen

So zeigen Sie eine Liste mit sekundären (einschl. virtuellen) Administrationsservern an:

1. Wählen Sie im Hauptmenü einen beliebigen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**).
2. Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

Im neuen Navigationsbereich wird die Liste der sekundären (einschließlich virtueller) Administrationsserver angezeigt. Sie können auf den Namen eines dieser Administrationsserver klicken, um zu ihm zu wechseln.

Sie können nicht zu virtuellen Administrationsservern wechseln, wenn Sie den Navigationsbereich über die Abschnitte **IP-Bereiche** und **Gelöschte Objekte** geöffnet haben.
Die Administrationsgruppen werden ebenfalls angezeigt. Die Gruppen stehen zur Verwaltung zur Verfügung, wenn Sie den Navigationsbereich über einen der folgenden Abschnitte geöffnet haben: **Assets (Geräte)**, **Richtlinien**, **Aufgaben** und **Verteilungspunkte**. Andernfalls sind die Gruppen ausgegraut.

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 auf den Namen des primären Administrationsservers.
2. Wechseln 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.

Konfiguration der Schnittstelle

Sie können die Benutzeroberfläche der Kaspersky Next Expert View so konfigurieren, dass Abschnitte und Elemente der Benutzeroberfläche abhängig von den von Ihnen verwendeten Funktionen ein- und ausgeblendet werden.

So konfigurieren Sie die Benutzeroberfläche der Kaspersky Next Expert View gemäß den derzeit verwendeten Funktionen:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Einstellungen der Benutzeroberfläche**.
2. Aktivieren oder deaktivieren Sie im folgenden Fenster **Einstellungen der Benutzeroberfläche** die Optionen:

   - **Verschlüsselung und Datenschutz anzeigen**

     Sie können diese Option zum Anzeigen oder Verbergen des Abschnitts **Vorgänge** → **Verschlüsselung und Datenschutz** in der Benutzeroberfläche verwenden. Kaspersky Next Expert View speichert den Wert dieser Option nur für Ihr eigenes Benutzerkonto, während die anderen Benutzer einen anderen Wert einstellen können.

   - **Funktionen von MDR anzeigen**

     Sie können diese Option zum Anzeigen oder Verbergen des Abschnitts **Überwachung** → **Vorfälle** in der Benutzeroberfläche verwenden. Kaspersky Next Expert View speichert den Wert dieser Option nur für Ihr eigenes Benutzerkonto, während die anderen Benutzer einen anderen Wert einstellen können.

3. Geben Sie die Anzahl der Geräte an, die Kaspersky Next Expert View unter Ergebnisse der Richtlinienverteilung anzeigt.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Einstellungen der Benutzeroberfläche wurden Ihren Bedürfnissen entsprechend angepasst.

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.

Um einen virtuellen Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
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.
4. Klicken Sie in der Menüleiste auf **Neuer virtueller Administrationsserver**.
5. Geben Sie auf der nächsten Seite auf die Registerkarte folgendes an: **Name des virtuellen Administrationsservers**.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Der neue virtuelle Administrationsserver wird erstellt, zur Administrationsgruppe hinzugefügt und auf der Registerkarte **Administrationsserver** angezeigt.

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.

Um einen virtuellen Administrationsserver zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
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 nicht in der Liste **Zugriffsrechte** in den Eigenschaften des primären Administrationsservers enthalten ist.

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

Stellen Sie bei der Zuweisung eines Administrators sicher, dass Sie ihm den Zugriff nur auf einen einzigen virtuellen Administrationsserver gewähren. Ein Administrator mit Zugriff auf mehrere virtuelle Administrationsserver kann sich nicht an der Kaspersky Next Expert View anmelden.

Ein Administrator eines virtuellen Administrationsservers meldet sich an der Kaspersky Next Expert View genauso an, wie bei der Anmeldung am primären Administrationsserver. Kaspersky Next Expert View 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.
- Das erstellte Konto des Administrators des virtuellen Servers ist nicht in den Listen **Zugriffsrechte** in den Eigenschaften aller primärer und sekundärer Server enthalten.
- 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. Wechseln Sie zum erforderlichen virtuellen Administrationsserver:

   a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

   b. Klicken Sie im neuen Navigationsbereich auf den Namen des erforderlichen virtuellen Administrationsservers.

   > Aus den Abschnitten **IP-Bereiche** und **Gelöschte Objekte** können Sie nicht zu einem virtuellen Administrationsserver wechseln.

   Im Hauptmenü ändert sich der Administrationsserver zu dem von Ihnen ausgewählten.

2. Wechseln Sie zu den Eigenschaften des Administrationsservers, indem Sie im Hauptmenü auf dessen Namen klicken.

   Alternativ können Sie im Navigationsbereich den Mauszeiger über den Namen des virtuellen Administrationsservers bewegen und anschließend auf das Einstellungssymbol (⚙) klicken.

   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.

So weisen Sie mehreren virtuellen Administrationsservern einen Administrator zu:

1. Klicken Sie im Hauptmenü auf den Namen des primären Administrationsservers.

2. Wechseln Sie auf der angezeigten Seite zur Registerkarte **Zugriffsrechte** und klicken Sie anschließend auf **Zuweisen**.

   Aktivieren Sie im sich öffnenden Fenster „**Benutzer oder Gruppen hinzufügen**“ das Kontrollkästchen neben dem Benutzer, den Sie als Administrator zuweisen möchten.

3. Sie können zur Registerkarte „**Gruppen**“ wechseln, um die Benutzergruppen auszuwählen.

4. Klicken Sie auf die Schaltfläche **Weiter**.

5. Wählen Sie die Server aus, denen Sie einen Administrator zuweisen möchten, und klicken Sie anschließend auf **Weiter**.

   Bei Auswahl von zwei oder mehr virtuellen Servern wird automatisch der Zugriff auf deren primären Administrationsserver gewährt. In diesem Fall kann diese Auswahl nicht aufgehoben werden, ohne die Auswahl der virtuellen Server zu löschen.

6. Wählen Sie bei Bedarf die Administratorrollen aus, die Sie für den Benutzer festlegen möchten.

   Wenn Sie für den Benutzer benutzerdefinierte Rollen für den aktuellen Administrationsserver festlegen möchten, wechseln Sie zu den Eigenschaften des erforderlichen Administrationsservers, klicken Sie auf **Rollen festlegen** und wählen Sie anschließend die benutzerdefinierten Rollen aus.

7. Klicken Sie auf **Fertigstellen**, um die Änderungen zu übernehmen.

Der Administrator mit den ausgewählten Rollen ist jetzt mehreren virtuellen Administrationsservern zugewiesen.

So entziehen Sie die Zugriffsrechte des Administrators:

1. Wechseln Sie zum erforderlichen virtuellen Administrationsserver.

2. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

3. Wechseln Sie auf der nächsten Seite auf die Registerkarte „**Zugriffsrechte**“.

4. Aktivieren Sie das Kontrollkästchen neben dem Benutzer, dem Sie die Zugriffsrechte entziehen möchten.

5. Klicken Sie auf „**Widerrufen**“ und bestätigen Sie Ihre Aktion.

Die Zugriffsrechte des ausgewählten Benutzers werden entzogen.

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 zum erforderlichen virtuellen Administrationsserver:

   a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

   b. Klicken Sie im neuen Navigationsbereich auf den Namen des erforderlichen virtuellen Administrationsservers.

   > Aus den Abschnitten **IP-Bereiche** und **Gelöschte Objekte** können Sie nicht zu einem virtuellen Administrationsserver wechseln.

   Im Hauptmenü ändert sich der Administrationsserver zu dem von Ihnen ausgewählten.

3. Weisen Sie die neue Rolle oder mehrere Rollen dem Administratorkonto zu.

> Um einem Benutzer eine Rolle zuzuweisen, wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus. Wenn Sie die Registerkarte **Gruppen** auswählen und anschließend der Gruppe, in welcher sich der Benutzer befindet, Rollen zuweisen, kann sich der Benutzer nicht an Kaspersky Next Expert View anmelden.

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.

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 Next Expert View 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 den Administrationsserver.
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.

Überwachung und Berichterstattung

In diesem Abschnitt werden die Möglichkeiten für Monitoring und Berichte in Kaspersky Next Expert View beschrieben. Diese Möglichkeiten geben Ihnen einen Überblick über Ihre Infrastruktur, die Schutzstatus und Statistiken.

Nach der Bereitstellung von Kaspersky Next Expert View oder während des Programmbetriebs können Sie die Funktionen der Überwachung und Berichterstattung an Ihre Bedürfnisse anpassen.

Szenario: Überwachung und Berichterstattung

Dieser Abschnitt enthält ein Szenario zur Konfiguration der Funktion der Überwachung und Berichterstellung in Kaspersky Next Expert View.

Erforderliche Vorrausetzungen

Nach der Verteilung von Kaspersky Next Expert View im Unternehmensnetzwerk können Sie mit seiner Überwachung beginnen und Berichte zum Netzwerkbetrieb erstellen.

Schritte

Die Konfiguration der Überwachung und Berichterstellung in einem Unternehmensnetzwerk erfolgt in mehreren Etappen:

1. **Einstellungen zum Umschalten der Status von Geräten**

   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: Konfigurieren Sie Benachrichtigungen (per E-Mail) bei Ereignissen auf Client-Geräten

   > Zur langfristigen Speicherung der Ereignisse von Kaspersky-Anwendungen wird es empfohlen, die automatische Weiterleitung der Ereignisse an ein SIEM System zu konfigurieren. Dies ermöglicht auch schnelle E-Mail-Benachrichtigungen über Sicherheitsereignisse und eine schnellere Reaktion darauf.

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. **Sicherheitsstatus Ihres Unternehmensnetzwerks verfolgen**

   Anleitung:

   - Sehen Sie sich das **Schutzstatus** status an
   - **Bericht über den Schutzstatus** erstellen und überprüfen
   - **Fehlerbericht** erstellen und überprüfen

5. **Client-Geräte finden, die nicht geschützt sind**

   Anleitung:

   - Sehen Sie sich das Widget **Neue Geräte** an
   - **Bericht über die Bereitstellung des Schutzes** erstellen und überprüfen

6. **Schutz der Client-Geräte überprüfen**

   Anleitung:

   - Erstellen und lesen Sie Berichte der Kategorien **Schutzstatus** und **Bedrohungsstatistiken**
   - Starten und überprüfen Sie die Ereignisauswahl mit dem **Kritisch**-Wert

7. **Lizenzinformationen überprüfen**

   Anleitung:

   - Fügen Sie das Widget **Nutzung von Lizenzschlüsseln** zum Dashboard hinzu und sehen Sie es sich an
   - **Bericht über die Lizenzschlüsselnutzung** erstellen 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.

Arten der Überwachung und Berichterstattung

Die Informationen über die Sicherheitsereignisse im Unternehmensnetzwerk werden in der Administrationsserver-Datenbank gespeichert. Basierend auf den Ereignissen bietet die Kaspersky Next Expert View die folgenden Arten der Überwachung und Berichterstattung in Ihrem Unternehmensnetzwerk:

- Dashboard
- Berichte
- Ereignisauswahlen

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 Next Expert View verfügbar sind, erstellen und anzeigen.

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 Next Expert View in dem Abschnitt **Überwachung** 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 Next Expert View 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** → **Dashboard**.
2. Klicken Sie auf die Schaltfläche **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** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ausblenden möchten.
3. Wählen Sie **Widget ausblenden** 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** → **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** → **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** → **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:

- **Anwendungsbereich des 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.

- **Bekommt den Status "Kritisch" zugewiesen, wenn folgende Bedingungen erfüllt sind** und **Bekommt den Status "Warnung" zugewiesen, wenn folgende Bedingungen erfüllt sind** (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** → **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 Next Expert View 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 → 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 Next Expert View 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 Next Expert View 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 Next Expert View in dem Abschnitt **Überwachung** unter **Berichte**.

Standardmäßig enthalten Berichte Informationen für die letzten 30 Tage.

Die Kaspersky Next Expert View 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. Gehen Sie im Hauptmenü zu **Überwachung** → **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** → **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. Beachten Sie, dass beim Exportieren des Berichts in eine Datei diese Option keinen Einfluss auf die maximale Anzahl von aufzunehmenden Ereignissen hat.

       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.

       Die Benutzeroberfläche der Kaspersky Next Expert View kann maximal 2500 Einträge anzeigen. Wenn Sie eine größere Anzahl von Ereignissen anzeigen müssen, verwenden Sie die Funktion Bericht exportieren.
     - **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 regelmäßig 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.

Exportieren eines Berichts in eine Datei

Sie können einen oder mehrere Berichte im xml-, html- oder pdf-Format speichern. Mit Kaspersky Next Expert View können Sie bis zu 10 Berichte gleichzeitig in Dateien mit dem angegebenen Format exportieren.

So exportieren Sie einen Bericht in eine Datei:

1. Wechseln Sie im Hauptmenü zu **Überwachung → Berichte**.
2. Wählen Sie die Berichte aus, die Sie exportieren möchten.

   Wenn Sie mehr als 10 Berichte auswählen, wird die Schaltfläche **Bericht exportieren** deaktiviert.
3. Klicken Sie auf die Schaltfläche **Bericht exportieren**.

4. Geben Sie im geöffneten Fenster die folgenden Export-Einstellungen an:

   - **Dateiname**.

     Wenn Sie einen Bericht zum Exportieren auswählen, geben Sie den Dateinamen des Berichts an.

     Wenn Sie mehr als einen Bericht auswählen, stimmen die Namen der Berichtsdateien mit den Namen der ausgewählten Berichtsvorlagen überein.

   - **Maximale Anzahl an Einträgen**.

     Geben Sie die maximale Anzahl von Einträgen an, die in der Berichtsdatei enthalten sein sollen. Als Standardwert ist 10.000 vorgegeben.

   - **Dateiformat**.

     Wählen Sie das Dateiformat für den Bericht aus: XML, HTML oder PDF. Wenn Sie mehrere Berichte exportieren, werden alle ausgewählten Berichte im angegebenen Format als separate Dateien gespeichert.

5. Klicken Sie auf die Schaltfläche **Bericht exportieren**.

Der Bericht wird in einer Datei mit angegebenen Format gespeichert.

Bericht erstellen und anzeigen

Um einen Bericht zu erstellen und anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **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 ausschließlich auf Englisch angezeigt. Weitere Lokalisierungen sind nicht verfügbar.

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** → **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.

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. Dieser Parameter 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** → **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 Next Expert View auftretenden Ereignistypen, und zur Verwaltung der Blockierung häufiger Ereignisse.

Über die Ereignisse in Kaspersky Next Expert View

Kaspersky Next Expert View 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 den Gruppen der Geräte auftreten, operativ zu reagieren.

Ereignisse nach Typ

In Kaspersky Next Expert View gibt es 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.

Ereignisse nach Quelle

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.

Ereignisse können von den folgenden Programmen generiert werden:

- Komponenten der Kaspersky Next Expert View:
  - Administrationsserver
  - Administrationsagent
- Verwaltete Kaspersky-Anwendungen

  Weitere Informationen zu den Ereignissen, die von verwalteten Kaspersky-Anwendungen generiert werden, finden Sie in der Dokumentation der entsprechenden Anwendung.

Ereignisse nach Ereigniskategorie

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 Next Expert View 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.

Ereignisse von Kaspersky Next Expert View

Jede Komponente von Kaspersky Next Expert View hat einen eigenen Satz von Ereignistypen. Dieser Abschnitt enthält eine Liste mit Ereignissen, die auf dem Administrationsserver von Kaspersky Next Expert View und im Administrationsagenten 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 Next Expert View 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 durchsuchen und verarbeiten, und dafür die öffentlichen Ansichten nutzen, die von der Datenbank von Kaspersky Next Expert View bereitgestellt 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.

Ereignisse des Administrationsservers

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsserver beziehen.

Ereignisse des Administrationsservers: Kritisch

Die untenstehende Tabelle enthält die im Administrationsserver von Kaspersky Next Expert View vorkommenden Ereignisse 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** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. 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.

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Lizenzbeschränkung wurde überschritten	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Einmal pro Tag überprüft Kaspersky Next Expert View, ob eine Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, Lizenzbeschränkungen überschreiten. Außerdem treten die Ereignisse auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten, die von einer Lizenz abgedeckt 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 Next Expert View legt die Regeln fest, nach denen beim Überschreiten einer Lizenzbeschränkung Ereignisse generiert werden.	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
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

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
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
Eingeschränkter Funktionsmodus	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ereignisse dieser Art treten auf, wenn die Ausführung von Kaspersky Next Expert View mit grundlegenden Funktionen und ohne die Funktionen "Schwachstellen- und Patch-Management" und "Verwaltung mobiler Geräte" beginnt. Im Folgenden die Gründe für und geeignete Reaktionen auf das Ereignis: • Die Gültigkeitsdauer der Lizenz ist abgelaufen. Um den vollen Funktionsumfang von Kaspersky Next Expert View zu verwenden, stellen Sie eine Lizenz zur Verfügung (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

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
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 Next Expert View nur grundlegende Funktionen bereit. Sie können auf dieses Ereignis folgendermaßen reagieren: • Vergewissern Sie sich, dass ein Reserve-Lizenzschlüssel dem Administrationsserver 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
Das MDM-Zertifikat ist abgelaufen	4132	KLSRV_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn auf mobilen Geräten das Client-Zertifikat abläuft.	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 von Kaspersky Next Expert View und keine Module von Anwendungen, die durch Kaspersky verwaltet werden. 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 untenstehende Tabelle enthält die im Administrationsserver von Kaspersky Next Expert View vorkommenden Ereignisse 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** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. 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
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 Next Expert View die Lizenzschlüssel von Drittanbieter-Programmen verwalten und die Anzahl der Installationen das im Lizenzschlüssel des Drittanbieter-Programms festgelegte Limit überschreitet. 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-Anwendungen verwalten, indem Sie die Funktionen der lizenzierten Anwendungsgruppe 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

Ereignisse des Administrationsservers: Warnung

Die untenstehende Tabelle enthält die im Administrationsserver von Kaspersky Next Expert View vorkommenden Ereignisse 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** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. 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.

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Lizenzbeschränkung wurde überschritten	4098	KLSRV_EV_LICENSE_CHECK_100_110	Einmal pro Tag überprüft Kaspersky Next Expert View, ob eine Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, Lizenzbeschränkungen überschreiten. Außerdem treten die Ereignisse auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten, die von einer Lizenz abgedeckt 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 Cloud Console legt die Regeln fest, nach denen beim Überschreiten einer Lizenzbeschränkung Ereignisse generiert werden.	90 Tage
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 **mithilfe von Kaspersky Next Expert View** den Zeitraum an, nach dessen Ablauf das Ereignis Das Gerät war lange Zeit im Netzwerk inaktiv erstellt wird. • Geben Sie mithilfe von Kaspersky Next Expert View den Zeitraum an, nach dessen Ablauf das Gerät automatisch aus der Gruppe entfernt wird.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
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. Obwohl Klonen von Kaspersky Next Expert View nicht unterstützt wird, kann dieses Ereignis auftreten, wenn z. B. ein Drittanbieter-Tool zum Klonen verwendet wird. Um dieses Ereignis zu vermeiden, müssen Sie beim Kopieren eines Geräte-Images mit installiertem Administrationsagenten die folgenden Empfehlungen beachten: • Beenden Sie auf dem Referenzgerät den Dienst des Administrationsagenten und führen Sie das Tool "klmover" mit dem Parameter "-dupfix" aus. Vermeiden Sie die erneute Ausführung des Administrationsagent, bis der Vorgang zum Aufzeichnen des Images abgeschlossen ist. • Stellen Sie nach der Bereitstellung des Images beim ersten Start des Betriebssystems sicher, das vor dem ersten Starten des Administrationsagenten das Tool "klmover" mit dem Parameter "-dupfix" ausgeführt wird (zwingende Voraussetzung). Das Tool "klmover" ist Teil des Installationspakets des Administrationsagenten. Wenn Sie ein Geräte-Image ohne installierten Administrationsagenten aufzeichnen, rollen Sie das Image auf den Zielgeräten aus und stellen Sie anschließend den Administrationsagenten bereit. Dafür müssen Sie den Zugriff der Geräte auf den Netzwerkordner mit autonomen Installationspaketen gewähren.	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 erreicht	4127	KLSRV_INVLICPROD_FILLED	Ereignisse dieser Art treten auf, wenn die Anzahl der Installationen von Drittanbieter-Anwendungen, die in einer lizenzierten Anwendungsgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben 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 Drittanbieteranwendungen verwalten, indem Sie die Funktionen der lizenzierten Anwendungsgruppe 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 wurde angefordert** 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 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.	90 Tage
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.	90 Tage
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 Google 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 Google 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 Google 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 zurückgibt. 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 Google 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 des Ereignisses 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 Google 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
Häufige Ereignisse 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
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 Betriebssystem-Protokoll 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 Betriebssystem-Protokoll des Geräts, auf dem der primäre Administrationsserver installiert ist, und reagieren Sie entsprechend.	90 Tage
Audit: testweise Verbindung zu SIEM-Server fehlgeschlagen	5120	KLAUD_EV_SIEM_TEST_FAILED	Ereignisse dieser Art treten auf, wenn ein automatischer Verbindungstest mit dem SIEM-Server fehlgeschlagen ist.	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. Sie können diese Updates in der Kaspersky Security Center Web Console genehmigen 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 Datenbank des Administrationsservers begonnen hat, nachdem die Kapazitätsgrenze der Datenbank des Administrationsservers 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 Datenbank des Administrationsservers gelöscht wurden, nachdem die Kapazitätsgrenze der Datenbank des Administrationsservers 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

Ereignisse des Administrationsservers: Information

Die untenstehende Tabelle enthält die im Administrationsserver von Kaspersky Next Expert View vorkommenden Ereignisse 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** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. 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	Beschreibung	Standard-Speicherdauer
Der Lizenzschlüssel ist zu über 90% verbraucht	4097	KLSRV_EV_LICENSE_CHECK_90	Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, Lizenzbeschränkungen fast überschreiten. Außerdem treten die Ereignisse auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten, die von einer Lizenz abgedeckt werden, mehr als 90% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Die Client-Geräte sind selbst dann geschützt, wenn eine Lizenzbeschränkung überschritten wird. 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 Next Expert View legt die Regeln fest, nach denen beim Überschreiten einer Lizenzbeschränkung Ereignisse generiert werden.	30 Tage
Neues Gerät wurde erkannt	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Ereignisse dieser Art treten auf, wenn im Netzwerk neue Geräte entdeckt wurden.	30 Tage
Das Gerät wurde entsprechend einer Regel automatisch verschoben	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Ereignisse dieser Art treten auf, wenn Geräte gemäß den Regeln für das Verschieben von Geräten einer Gruppe zugewiesen wurden.	30 Tage
Das Gerät wurde aus der Gruppe gelöscht: Lange Zeit im Netzwerk inaktiv	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Ereignisse dieser Art treten auf, wenn Geräte aufgrund von Inaktivität automatisch aus einer Gruppe entfernt wurden.	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Beschränkung für die Anzahl von Installationen wird für eine der lizenzierten Programmgruppen bald überschritten (mehr als 90% verbraucht)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Ereignisse dieser Art treten auf, wenn die Anzahl der Installationen von Dritthersteller-Programmen, die in einer lizenzierten Programmgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben 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.	30 Tage
Es wurden Dateien gefunden, die zur Analyse an Kaspersky gesendet werden	4131	KLSRV_APS_FILE_APPEARED		30 Tage
Die FCM Instance ID hat sich auf diesem mobilen Gerät geändert	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Ereignisse dieser Art treten auf, wenn sich der Token von Firebase Cloud Messaging auf dem Gerät geändert hat. Informationen zur Rotation des FCM-Tokens finden Sie in der Dokumentation des Firebase-Dienstes.	30 Tage
Updates wurden erfolgreich in den angegebenen Ordner kopiert	4122	KLSRV_UPD_REPL_OK	Ereignisse dieser Art treten ein, wenn die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** das Kopieren der Dateien in den angegebenen Ordner abgeschlossen hat.	30 Tage
Die Verbindung mit dem sekundären Administrationsserver wurde hergestellt	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Weitere Informationen dazu finden Sie in diesem Thema: Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen.	30 Tage
Die Verbindung mit dem primären Administrationsserver wurde hergestellt	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 Tage
Datenbanken wurden aktualisiert (In Kaspersky Next Expert View ist dieser Ereignistyp nur für einen sekundären Administrationsserver verfügbar.)	4144	KLSRV_UPD_BASES_UPDATED	Ereignisse dieser Art treten ein, wenn die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** das Aktualisieren der Datenbanken abgeschlossen hat.	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Gerät wurde automatisch zur Gruppe hinzugefügt	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Ereignisse dieser Art treten auf, wenn Geräte gemäß den Regeln für das Verschieben von Geräten einer Gruppe zugewiesen wurden.	30 Tage
KSN-Proxy wurde gestartet. Überprüfen der KSN-Verfügbarkeit wurde erfolgreich abgeschlossen	7718	KSNPROXY_STARTED_CON_CHK_OK		30 Tage
KSN-Proxy wurde angehalten	7720	KSNPROXY_STOPPED		30 Tage
Audit: Verbindung mit dem Administrationsserver wurde hergestellt	4147	KLAUD_EV_SERVERCONNECT		30 Tage
Audit: Die Verbindung mit dem Administrationsserver wurde unterbrochen	4151	KLAUD_EV_SERVERDISCONNECT		30 Tage
Audit: Objekt wurde geändert	4148	KLAUD_EV_OBJECTMODIFY	Dieses Ereignis verfolgt Änderungen in den folgenden Objekten: • Administrationsgruppe • Sicherheitsgruppe • Benutzer • Paket • Aufgabe • Richtlinie • Server • Virtueller Server	30 Tage
Audit: Objekteigenschaften wurden geändert	4152	KLAUD_EV_OBJECTPROPMODIFIED	Dieses Ereignis verfolgt Änderungen der folgenden Eigenschaften: • Benutzer • Lizenz • Server • Virtueller Server	30 Tage
Audit: Objektstatus geändert	4150	KLAUD_EV_TASK_STATE_CHANGED	Dieses Ereignis tritt beispielsweise auf, wenn eine Aufgabe mit einem Fehler beendet wurde.	30 Tage
Audit: Gruppeneinstellungen modifiziert	4149	KLAUD_EV_ADMGROUP_CHANGED	Ereignisse dieser Art treten auf, wenn eine Sicherheitsgruppe bearbeitet wurde.	30 Tage
Audit: Die Chiffrierschlüssel wurden vom Administrationsserver importiert oder exportiert	5100	KLAUD_EV_DPEKEYSEXPORT		30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Audit: testweise Verbindung zu SIEM-Server erfolgreich	5110	KLAUD_EV_SIEM_TEST_SUCCESS		30 Tage
Audit: Benutzerberechtigungen wurden geändert	4153	KLAUD_EV_OBJECTACLMODIFIED	Dieses Ereignis tritt auf, wenn Benutzerberechtigungen geändert wurden.	30 Tage

Ereignisse des Administrationsagenten

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsagenten beziehen.

Ereignisse des Administrationsagenten: Funktionsfehler

Die nachfolgende Tabelle enthält die Ereignisse 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 das Patchen von Komponenten von Kaspersky Next Expert View nicht erfolgreich waren. 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 eines Drittanbieter-Programms 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
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
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
Benutzerverwaltung: Fehler	7723	KLNAG_EV_USR_MNG_ERR	Ereignis bei einer allgemeinen Warnung.	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
Ein Sicherheitsvorfall ist eingetreten	549	GNRL_EV_APP_INCIDENT_OCCURED	30 Tage
Die gefundene sudoers-Datei entspricht nicht dem Referenzwert	7724	KLNAG_EV_SUDOER_DIFFERENT	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

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 für Software-Module 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
Root-Zertifikate wurden installiert	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 Tage
Root-Zertifikate wurden entfernt	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 Tage
Sudoers-Datei wurde erfolgreich auf Referenzwert zurückgesetzt	7725	KLNAG_EV_SUDOER_RESTORED	30 Tage
Neues Gerät wurde hinzugefügt	7708	KLNAG_EV_DEVICE_ARRIVAL	30 Tage
Gerät wurde entfernt	7709	KLNAG_EV_DEVICE_REMOVE	30 Tage
Gerät wurde erkannt	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 Tage
Gerät wurde autorisiert	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 Tage
Benutzerverwaltung: Informationen	7721	KLNAG_EV_USR_MNG_INF	30 Tage
Webserver wurde auf dem Host gestartet	—	WEB_SERVER_STARTED	30 Tage
Webserver wurde auf dem Host gestoppt	—	WEB_SERVER_STOPPED	30 Tage
Zertifikat des HTTPS-Ports des Webservers wurde abgerufen	—	WEB_SERVER_CERTIFICATE_RENEWED	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: Bereitgestellt	7715	KLUSRLOG_EV_WDS_BEGIN	30 Tage
Windows Desktopfreigabe: Abgeschlossen	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

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
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

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 Next Expert View verfügbar sind, erstellen und anzeigen.

Ereignisauswahlen finden Sie in Kaspersky Next Expert View in dem Abschnitt **Überwachung** unter **Ereignisauswahlen**.

Standardmäßig enthalten Ereignisauswahlen Informationen für die letzten sieben Tage.

Kaspersky Next Expert View 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

  In Kaspersky Next Expert View werden Audit-Ereignisse für Dienstvorgänge in Ihrem Arbeitsbereich angezeigt. Diese Ereignisse werden durch Aktionen von Kaspersky-Spezialisten ausgelöst. Beispiele für solche Ereignisse: Ändern der Administrationsserver-Ports; Backup der Administrationsserver-Datenbank; Erstellen, Ändern und Löschen von Benutzerkonten.

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 Next Expert View 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** → **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 Ergebnis der Auswahl wechseln** aktiviert.
6. Klicken Sie auf **Speichern**, um die Erstellung der Ereignisauswahl zu bestätigen.

Wenn Sie das Kontrollkästchen **Zum Ergebnis der Auswahl 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** → **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** → **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 Next Expert View 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 Next Expert View (vordefinierte Auswahlen) können nicht in einer Datei gespeichert werden.

So exportieren Sie eine Ereignisauswahl:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **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 Next Expert View 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** → **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 Next Expert View 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.

Für Aufgaben und Richtlinien Informationen über Ereignisse protokollieren

Dieser Abschnitt enthält Empfehlungen zur Minimierung der Anzahl von Ereignissen für Aufgaben und Richtlinien, die in der Datenbank der Kaspersky Next Expert View gespeichert sind. Wenn das Speicherlimit überschritten wird, werden alte Ereignisse durch neue überschrieben. Dadurch können kritische Ereignisse verloren gehen. Darüber hinaus kann auf dem Administrationsserver das Ereignis mit der Warnung **Die Maximalanzahl an Ereignissen in der Datenbank wurde überschritten. Die Ereignisse wurden gelöscht** auftreten. In diesen Fällen empfehlen wir Ihnen, die Anweisungen in diesem Abschnitt zu befolgen.

Dadurch erhöhen Sie die Performance von Szenarien, die mit der Analyse von Ereignissen verbunden sind. Darüber hinaus helfen Ihnen diese Empfehlungen bei der Verringerung des Risikos, dass kritische Ereignisse von einer großen Anzahl an Ereignissen überschrieben werden.

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 häufig ausgeführt wird (z. B. mehr als einmal pro Woche), kann sich eine große Anzahl an Ereignissen ansammeln, welche die Datenbank überfüllen. In einem solchen Fall empfehlen wir, in den Eigenschaften der Aufgabe eine von zwei Optionen festzulegen:

- **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**. In diesem Fall werden 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) von Kaspersky Next Expert View gespeichert.
- **Nur die Ergebnisse der Aufgabenausführung speichern**. In diesem Fall werden von jedem Gerät, auf dem die Aufgabe ausgeführt wird, nur Informationen über den Abschluss der Aufgabe (erfolgreich, mit Warnung oder mit einem Fehler) von Kaspersky Next Expert View gespeichert.

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 empfehlen wir, in den Eigenschaften der Richtlinie nur die kritischsten Ereignisse auszuwählen und deren Protokollierung zu aktivieren. Es wird empfohlen, die Speicherung aller anderen Ereignisse zu deaktivieren.

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.

Es ist ratsam, die Einstellungen der Ereignisspeicherung zu ändern, wenn Ereignisse über Änderungen des Zwischenstatus von Gruppenaufgaben oder über die Anwendung von Richtlinien einen großen Anteil aller Ereignisse in der Datenbank der Kaspersky Next Expert View einnehmen.

Ereignisse löschen

So löschen Sie Ereignisse aus einer Ereignisauswahl:

1. Starten einer Ereignisauswahl.
2. Wählen Sie die Ereignisse aus:
   - Aktivieren Sie die Kontrollkästchen neben allen Ereignissen, die Sie löschen möchten.
   - Wenn Sie alle Ereignisse auf der aktuellen Seite löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste mit den Ereignissen und klicken Sie auf die Option **Alle auf aktueller Seite auswählen**.
   - Wenn Sie alle Ereignisse aus einer Auswahl löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste und klicken Sie auf die Option **Alle auswählen**.
3. Klicken Sie auf die Schaltfläche **Löschen**.

So löschen Sie Ereignisse aus einer Liste mit Geräteereignissen:

1. Öffnen Sie die Geräteliste.
   - Für verwaltete Geräte: **Asset-Verwaltung** → **Assets (Geräte)**.
   - Für nicht zugeordnete Geräte: **Gerätesuche und Bereitstellung** → **Nicht zugeordnete Geräte**.
2. Klicken Sie in der Geräteliste auf den Link mit dem Namen des gewünschten Geräts und wechseln Sie anschließend zur Registerkarte **Ereignisse**.
3. Wählen Sie die Ereignisse aus:
   - Aktivieren Sie die Kontrollkästchen neben allen Ereignissen, die Sie löschen möchten.
   - Wenn Sie alle Ereignisse auf der aktuellen Seite löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste mit den Ereignissen und klicken Sie auf die Option **Alle auf aktueller Seite auswählen**.
   - Wenn Sie alle Ereignisse aus einer Auswahl löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste und klicken Sie auf die Option **Alle auswählen**.
4. 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** → **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.

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.

Über Benachrichtigungen

Benachrichtigungen informieren Sie über wichtige Ereignisse und helfen Ihnen, schnell darauf zu reagieren, indem Sie die empfohlenen oder andere geeignete Aktionen ausführen.

Abhängig von der ausgewählten Benachrichtigungsmethode sind folgende Benachrichtigungstypen verfügbar:

- Bildschirmbenachrichtigungen
- E-Mail-Benachrichtigungen

Bildschirmbenachrichtigungen

Bildschirmbenachrichtigungen sind im Dropdown-Bereich, der durch Klicken auf das Benachrichtigungssymbol ( ) geöffnet wird, und in der Mitteilungszentrale verfügbar. Sie werden einer der folgenden Kategorien zugeordnet: **Kritisch**, **Warnung** oder **Information**.

Wenn das Benachrichtigungssymbol einen roten Punkt aufweist, liegen ungelesene Benachrichtigungen vor.

Bildschirmbenachrichtigungen werden in folgende Typen unterteilt:

- **Erfordert Ihre Aufmerksamkeit**

  Benachrichtigungen, die Ihre Aufmerksamkeit erfordern. Benachrichtigungen der Kategorie **Kritisch** werden zusätzlich zur Mitteilungszentrale auf dem Haupt-Dashboard angezeigt.

- **System**

  Systembenachrichtigungen. Sie sind in folgende Kategorien unterteilt:

  - **Bereitstellung**
  - **Geräte**
  - **Schutz**
  - **Updates** (umfasst Benachrichtigungen über zum Download verfügbare Kaspersky-Anwendungen, über heruntergeladene Updates für die Antiviren-Datenbanken sowie über Geräte (falls vorhanden), die nach einem Update des Administrationsagenten neu gestartet werden müssen)
  - **Exploit-Prävention**
  - **Administrationsserver** (umfasst nur Ereignisse, die den Administrationsserver betreffen)

- **Ankündigungen**

  Benachrichtigungen mit Informationen zu Ihrer Version von Kaspersky Next Expert View und zu den verwalteten Anwendungen, die auf den verwalteten Geräten installiert sind.

Sie können Ihr Unternehmensnetzwerk überwachen, indem Sie Bildschirmbenachrichtigungen anzeigen und in Echtzeit darauf reagieren.

E-Mail-Benachrichtigungen

Kaspersky Next Expert View bietet die Möglichkeit, Ihr Unternehmensnetzwerk zu kontrollieren, indem über alle Ereignisse, die Sie als wichtig einstufen, Benachrichtigungen versandt werden. Sie können für jedes Ereignis Benachrichtigungen per E-Mail konfigurieren.

Nach dem Erhalten von Benachrichtigungen per E-Mail können Sie entscheiden, wie Sie auf das Ereignis reagieren. Diese Reaktion sollte für Ihr Unternehmensnetzwerk am besten geeignet sein.

Anzeigen von Benachrichtigungen, die Ihre Aufmerksamkeit erfordern

Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, informieren Sie über Ereignisse, die möglicherweise Ihr Eingreifen erfordern. Ihnen wird eine der folgenden Wichtigkeitskategorien zugewiesen: **Kritisch**, **Warnung** oder **Information**.

Benachrichtigungen der Kategorie **Kritisch** werden zusätzlich zur Mitteilungszentrale in der Web Console angezeigt. Wenn mehrere kritische Benachrichtigungen vorliegen, zeigt die Web Console eine einzige Benachrichtigung mit der Gesamtzahl der kritischen Benachrichtigungen an.

Sie können Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, auf eine der folgenden Arten anzeigen:

- Im Dropdown-Bereich

  Im Dropdown-Bereich werden nur ungelesene Benachrichtigungen angezeigt, die Ihre Aufmerksamkeit erfordern. Wenn keine ungelesenen Benachrichtigungen vorliegen, die Ihre Aufmerksamkeit erfordern, wird die Registerkarte **Erfordert Ihre Aufmerksamkeit** nicht angezeigt.

- In der Mitteilungszentrale

  In der Mitteilungszentrale werden alle Benachrichtigungen angezeigt, die Ihre Aufmerksamkeit erfordern, einschließlich gelesener und ungelesener Benachrichtigungen. Wenn keine Benachrichtigungen vorliegen, die Ihre Aufmerksamkeit erfordern, wird die Registerkarte **Erfordert Ihre Aufmerksamkeit** nicht angezeigt.

So zeigen Sie Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, im Dropdown-Bereich an:

1. Klicken Sie oben in der Web Console auf das Benachrichtigungssymbol ( ).

   Der Dropdown-Bereich **Benachrichtigungen** wird geöffnet.

2. Zeigen Sie auf der Registerkarte **Erfordert Ihre Aufmerksamkeit** die ungelesenen Benachrichtigungen an.

3. Markieren Sie bei Bedarf Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, auf eine der folgenden Arten als gelesen:

   - Um eine Benachrichtigung als gelesen zu markieren, klicken Sie neben der Benachrichtigung auf das Schließen-Symbol (×).

   - Um alle Benachrichtigungen als gelesen zu markieren, klicken Sie auf **Alle als gelesen markieren**.

   Nachdem Sie die Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, überprüft und als gelesen markiert haben, wird die Registerkarte **Erfordert Ihre Aufmerksamkeit** im Dropdown-Bereich **Benachrichtigungen** nicht mehr angezeigt. Sie können alle gelesenen Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, in der Mitteilungszentrale anzeigen.

So zeigen Sie Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, in der Mitteilungszentrale an:

1. Klicken Sie oben in der Web Console auf das Benachrichtigungssymbol ( ).

2. Klicken Sie im daraufhin geöffneten Dropdown-Bereich **Benachrichtigungen** auf die Schaltfläche **Zur Benachrichtigungszentrale wechseln**.

   Das Fenster **Benachrichtigungszentrale** wird geöffnet.

3. Wählen Sie auf der Registerkarte **Erfordert Ihre Aufmerksamkeit** einen der folgenden Abschnitte aus:

   - **Alle Benachrichtigungen, die Ihre Aufmerksamkeit erfordern** – Zeigt alle Benachrichtigungen an, die Ihre Aufmerksamkeit erfordern, unabhängig von ihrer Kategorie.
   - **Kritisch** – Zeigt Benachrichtigungen der Kategorie **Kritisch** an.
   - **Warnung** – Zeigt Benachrichtigungen der Kategorie **Warnung** an.
   - **Information** – Zeigt Benachrichtigungen der Kategorie **Information** an.

4. Um nur ungelesene Benachrichtigungen anzuzeigen, aktivieren Sie den Schalter **Nur ungelesene anzeigen**.
5. Klicken Sie in der Benachrichtigungsliste auf eine Benachrichtigung, um deren Text anzuzeigen. Die vollständige Benachrichtigung wird rechts im Detailbereich angezeigt.

   Wenn Sie eine Benachrichtigung anzeigen, wird sie automatisch als gelesen markiert.
6. Um Benachrichtigungen manuell als gelesen zu markieren, führen Sie eine der folgenden Aktionen aus:

   - Um eine Benachrichtigung als gelesen zu markieren, wählen Sie sie in der Benachrichtigungsliste aus und klicken Sie anschließend auf die Schaltfläche **Als gelesen markieren**.
   - Um alle Benachrichtigungen als gelesen zu markieren, klicken Sie auf die Schaltfläche **Alle als gelesen markieren**.

7. Bei Bedarf können Sie eine Benachrichtigung als ungelesen markieren, indem Sie sie in der Benachrichtigungsliste auswählen und anschließend auf die Schaltfläche **Als ungelesen markieren** klicken.

Benachrichtigungen, die Ihre Aufmerksamkeit erfordern, werden überprüft.

Systembenachrichtigungen anzeigen

Systembenachrichtigungen informieren Sie über Ereignisse im Zusammenhang mit der Web Console und verwalteten Geräten. Systembenachrichtigungen werden nach Typ gruppiert und einer der folgenden Wichtigkeitskategorien zugeordnet: **Kritisch**, **Warnung** oder **Information**.

Sie können Systembenachrichtigungen auf eine der folgenden Arten anzeigen:

- Im Dropdown-Bereich
- In der Mitteilungszentrale

So zeigen Sie Systembenachrichtigungen im Dropdown-Bereich an:

1. Klicken Sie oben in der Web Console auf das Benachrichtigungssymbol ( ).

   Der Dropdown-Bereich **Benachrichtigungen** wird geöffnet.
2. Zeigen Sie auf der Registerkarte **System** die ungelesenen Benachrichtigungen an.

3. Markieren Sie Systembenachrichtigungen bei Bedarf auf eine der folgenden Arten als gelesen:

   - Um eine Benachrichtigung als gelesen zu markieren, klicken Sie neben der Benachrichtigung auf das Symbol zum Schließen (×).
   - Um alle Benachrichtigungen als gelesen zu markieren, klicken Sie auf **Alle als gelesen markieren**.

   Nachdem Sie alle Systembenachrichtigungen überprüft und als gelesen markiert haben, wird im Dropdown-Bereich **Benachrichtigungen** eine Meldung angezeigt, dass keine neuen Benachrichtigungen vorhanden sind. Sie können alle Systembenachrichtigungen, einschließlich der gelesenen und ungelesenen Benachrichtigungen, in der Mitteilungszentrale anzeigen.

So zeigen Sie Systembenachrichtigungen in der Mitteilungszentrale an:

1. Klicken Sie oben in der Web Console auf das Benachrichtigungssymbol ( ).
2. Klicken Sie im daraufhin geöffneten Dropdown-Bereich **Benachrichtigungen** auf die Schaltfläche **Zur Benachrichtigungszentrale wechseln**.

   Das Fenster **Benachrichtigungszentrale** wird geöffnet.
3. Wählen Sie auf der Registerkarte **System** einen der folgenden Abschnitte aus:

   - **Alle Systembenachrichtigungen**
   - **Bereitstellung**
   - **Geräte**
   - **Schutz**
   - **Updates**
   - **Exploit-Prävention**
   - **Administrationsserver**
4. Um nur ungelesene Benachrichtigungen anzuzeigen, aktivieren Sie den Schalter **Nur ungelesene anzeigen**.
5. Klicken Sie in der Benachrichtigungsliste auf eine Benachrichtigung, um deren Meldung anzuzeigen. Die vollständige Benachrichtigung wird im Detailbereich auf der rechten Seite angezeigt.

   Wenn Sie eine Benachrichtigung anzeigen, wird sie automatisch als gelesen markiert.
6. Um Benachrichtigungen manuell als gelesen zu markieren, führen Sie eine der folgenden Aktionen aus:

   - Um eine Benachrichtigung als gelesen zu markieren, wählen Sie sie in der Benachrichtigungsliste aus und klicken Sie dann auf die Schaltfläche **Als gelesen markieren**.
   - Um alle Benachrichtigungen als gelesen zu markieren, klicken Sie auf die Schaltfläche **Alle als gelesen markieren**.
7. Bei Bedarf können Sie eine Benachrichtigung als ungelesen markieren, indem Sie sie in der Benachrichtigungsliste auswählen und dann auf die Schaltfläche **Als ungelesen markieren** klicken.

Systembenachrichtigungen werden überprüft.

Anzeigen von Mitteilungen

Mitteilungen sind eine Art von Benachrichtigung, die Informationen über Ihre Version von Kaspersky Next Expert View und die auf Ihren verwalteten Geräten installierten Kaspersky-Anwendungen bereitstellt. Es werden nur Mitteilungen angezeigt, die für den derzeit verbundenen Administrationsserver und die auf den verwalteten Geräten dieses Administrationsservers installierten Kaspersky-Anwendungen relevant sind. Mitteilungen werden für jeden Administrationsserver separat angezeigt, unabhängig davon, ob es sich um einen primären, sekundären oder virtuellen Administrationsserver handelt.

Wenn Kaspersky Next Expert View von mehreren Administratoren verwendet wird und diese unterschiedliche Sprachen für die Benutzeroberfläche einstellen, zeigt Kaspersky Next Expert View die Kaspersky-Mitteilungen in allen von den Administratoren verwendeten Sprachen an. Wenn Sie die Sprache der Benutzeroberfläche ändern, werden automatisch die Kaspersky-Mitteilungen in der ausgewählten Sprache zum Abschnitt hinzugefügt, nachdem Sie sich von der Web Console abgemeldet und erneut angemeldet haben.

Mitteilungen enthalten die folgenden Arten von Informationen:

- Sicherheitsrelevante Informationen

  Sicherheitsrelevante Mitteilungen umfassen kritische Updates, das Schließen von Schwachstellen und Empfehlungen zum Beheben von Problemen in Kaspersky-Anwendungen. Sicherheitsrelevante Mitteilungen sind standardmäßig aktiviert. Wenn Sie keine sicherheitsrelevanten Mitteilungen erhalten möchten, können Sie diese Funktion deaktivieren.

  Im Testmodus von Kaspersky Next Expert View können Sie die sicherheitsrelevanten Mitteilungen nicht deaktivieren.

  Um Informationen bereitzustellen, die für die Konfiguration Ihres Netzwerkschutzes relevant sind, sendet Kaspersky Next Expert View Daten an die Kaspersky-Cloud-Server und empfängt nur Mitteilungen zu den in Ihrem Netzwerk installierten Kaspersky-Anwendungen. Die Daten, die an die Server gesendet werden können, sind im Endbenutzer-Lizenzvertrag beschrieben, den Sie bei der Installation von Kaspersky Next Expert View akzeptieren.

- Marketinginformationen

  Marketing-Mitteilungen umfassen Sonderangebote, Produktneuigkeiten und Werbung für Kaspersky-Anwendungen. Marketing-Mitteilungen sind nur verfügbar, wenn Kaspersky Security Network (KSN) aktiviert ist. Sie können Marketing-Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

  Um Informationen bereitzustellen, die Ihnen beim Schutz Ihrer Netzwerkgeräte und bei der Erledigung alltäglicher Aufgaben helfen können, sendet Kaspersky Next Expert View Daten an die Kaspersky-Cloud-Server und empfängt relevante Mitteilungen. Die Daten, die an die Server gesendet werden können, werden im Abschnitt "Verarbeitete Daten" der KSN-Erklärung beschrieben.

Mitteilungen werden einer der folgenden Wichtigkeitskategorien zugeordnet: **Kritisch**, **Warnung** oder **Information**.

Sie können Mitteilungen auf eine der folgenden Arten anzeigen:

- Im Dropdown-Bereich
- In der Mitteilungszentrale

So zeigen Sie Mitteilungen im Dropdown-Bereich an:

1. Klicken Sie oben in der Web Console auf das Benachrichtigungssymbol ( ).

   Der Dropdown-Bereich **Benachrichtigungen** wird geöffnet.

2. Zeigen Sie auf der Registerkarte **Ankündigungen** ungelesene Benachrichtigungen an.

3. Markieren Sie Benachrichtigungen bei Bedarf auf eine der folgenden Arten als gelesen:

   - Um eine Benachrichtigung als gelesen zu markieren, klicken Sie neben der Benachrichtigung auf das Symbol zum Schließen (×).

   - Um alle Benachrichtigungen als gelesen zu markieren, klicken Sie auf **Alle als gelesen markieren**.

Nachdem Sie alle Benachrichtigungen geprüft und als gelesen markiert haben, wird im Dropdown-Bereich **Benachrichtigungen** eine Meldung angezeigt, dass keine neuen Benachrichtigungen vorhanden sind. Sie können alle Benachrichtigungen, sowohl gelesene als auch ungelesene, in der Mitteilungszentrale anzeigen.

So zeigen Sie Mitteilungen in der Mitteilungszentrale an:

1. Klicken Sie oben in der Web Console auf das Benachrichtigungssymbol ( ).

2. Klicken Sie im daraufhin geöffneten Dropdown-Bereich **Benachrichtigungen** auf die Schaltfläche **Zur Benachrichtigungszentrale wechseln**.

   Das Fenster **Benachrichtigungszentrale** wird geöffnet.

3. Wählen Sie auf der Registerkarte **Ankündigungen** einen der folgenden Abschnitte aus:

   - **Alle Ankündigungen** – Zeigt alle Benachrichtigungen unabhängig von ihrer Kategorie an.

   - **Kritisch** – Zeigt Benachrichtigungen der Kategorie **Kritisch** an.

   - **Warnung** – Zeigt Benachrichtigungen der Kategorie **Warnung** an.

   - **Information** – Zeigt Benachrichtigungen der Kategorie **Information** an.

4. Um nur ungelesene Benachrichtigungen anzuzeigen, aktivieren Sie den Schalter **Nur ungelesene anzeigen**.

5. Klicken Sie in der Benachrichtigungsliste auf eine Benachrichtigung, um deren Meldung anzuzeigen. Die vollständige Benachrichtigung wird im Detailbereich auf der rechten Seite angezeigt.

   Wenn Sie eine Benachrichtigung anzeigen, wird sie automatisch als gelesen markiert.

6. Um Benachrichtigungen manuell als gelesen zu markieren, führen Sie einen der folgenden Schritte aus:

   - Um eine Benachrichtigung als gelesen zu markieren, wählen Sie sie in der Benachrichtigungsliste aus und klicken Sie anschließend auf die Schaltfläche **Als gelesen markieren**.

   - Um alle Benachrichtigungen als gelesen zu markieren, klicken Sie auf die Schaltfläche **Alle als gelesen markieren**.

7. Bei Bedarf können Sie eine Benachrichtigung als ungelesen markieren, indem Sie sie in der Benachrichtigungsliste auswählen und anschließend auf die Schaltfläche **Als ungelesen markieren** klicken.

Ankündigungen werden überprüft.

Deaktivieren von Mitteilungen

Mitteilungen enthalten zwei Arten von Informationen:

- Sicherheitsrelevante Mitteilungen
- Marketing-Mitteilungen

Sie können jeden Mitteilungstyp getrennt deaktivieren.

Im Testmodus von Kaspersky Next Expert View können Sie die sicherheitsrelevanten Mitteilungen nicht deaktivieren.

Deaktivieren von sicherheitsrelevanten Mitteilungen

Um sicherheitsrelevante Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
   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**.
   Sicherheitsrelevante Mitteilungen sind deaktiviert.

Deaktivieren von Marketing-Mitteilungen

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 auf den Namen des Administrationsservers.
   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Einstellungen** aus.
3. Stellen Sie den Umschalter auf die Option **Kaspersky Security Network verwenden Deaktiviert**.

4. Klicken Sie auf die Schaltfläche **Speichern**.

   Jetzt sind die Marketing-Mitteilungen deaktiviert.

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 **Asset-Verwaltung → 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 **Bekommt den Status "Kritisch" zugewiesen, wenn folgende Bedingungen erfüllt sind** 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 **Asset-Verwaltung → 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 **Bekommt den Status "Warnung" zugewiesen, wenn folgende Bedingungen erfüllt sind** 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

In Kaspersky Next Expert View können Sie E-Mail-Benachrichtigung über auftretende Ereignisse konfigurieren.

So können Sie in Kaspersky Next Expert View Benachrichtigung über auftretende Ereignisse konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.
2. Wechseln Sie in den Abschnitt **Benachrichtigung** und geben Sie im rechten Fensterbereich die Einstellungen für die E-Mail-Benachrichtigung an:

   Empfänger (E-Mail-Adressen)

   Die E-Mail-Adressen der Nutzer, an die Kaspersky Next Expert View Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen.

   > Sie können maximal 24 E-Mail-Adressen angeben.
3. Klicken Sie auf die Schaltfläche **Testnachricht senden**, um zu prüfen, ob die Benachrichtigungen korrekt konfiguriert wurden: Das Programm sendet eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen.
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 Next Expert View auftreten.

Für die Einstellungen des Administrationsservers, einer Richtlinie oder des Programms können Sie im Abschnitt **Konfiguration von Ereignissen** die Benachrichtigungseinstellungen für bestimmte Ereignisse überschreiben.

Erhalten von Warnungen bei Ablauf der Lizenz

So fügen Sie dem Administrationsserver einen Lizenzschlüssel für Kaspersky Endpoint Security for Business Select hinzu:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel** aus.

3. Klicken Sie auf die Schaltfläche **Auswählen**.

4. Wählen Sie im folgenden Fenster Ihre Lizenz aus und klicken Sie auf **OK**.

   Wenn keine Lizenz angezeigt wird, können Sie alternativ auf **Neuen Lizenzschlüssel hinzufügen** klicken und Ihren Aktivierungscode verwenden.

Der Lizenz wird zur Datenverwaltung des Administrationsservers hinzugefügt. Dadurch generiert der Administrationsserver einen Tag vor Ablauf der Gültigkeitsdauer der Lizenz ein Kritisches Ereignis des Typs *Die Lizenz läuft bald ab.*, sowie anschließend ein kritisches Ereignis des Typs *Eingeschränkter Funktionsmodus*, wenn die Lizenz abgelaufen ist. Wenn Sie möchten, können Sie die Zustellung von Benachrichtigungen konfigurieren.

Wenn Sie der Datenverwaltung des Administrationsservers einen Lizenzschlüssel für Kaspersky Endpoint Security for Business Select hinzufügen, wird diese Lizenz als auf einem Gerät verwendet betrachtet.

Cloud Discovery

Kaspersky Next Expert View 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 Verwendung von Cloud-Diensten durch Schatten-IT zu erkennen und zu stoppen.

Diese Blockierfunktion ist nur verfügbar, wenn Sie Kaspersky Next Expert View unter einer Lizenz für Kaspersky Next EDR Optimum oder 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 für 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 Next Expert View 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 Widgets von Cloud Discovery:

1. Wechseln Sie zur Kaspersky Next Expert View.
2. Wechseln Sie im Hauptmenü zu **Überwachung → Dashboard**.
3. Klicken Sie im Widget **Cloud Discovery** auf die Schaltfläche **Aktivieren**.
4. Wählen Sie im folgenden Fenster **Cloud Discovery aktivieren** die Sicherheitsrichtlinien aus, für welche Sie die Funktion aktivieren möchten, und klicken Sie anschließend auf die Schaltfläche **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 zur Kaspersky Next Expert View.
2. Wechseln Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
3. Klicken Sie auf **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 Next Expert View erhält Informationen über die Nutzung von Cloud-Diensten von allen verwalteten Geräten, die nur durch die Sicherheitsprofile geschützt sind, bei denen diese Funktion aktiviert ist.

Stellen Sie vor dem Anzeigen sicher, dass:

- 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 Widget "Cloud Discovery" an:

1. Wechseln Sie zur Kaspersky Next Expert View.
2. Wechseln Sie im Hauptmenü zu **Überwachung** → **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** → **Berichte** wechseln, um die Berichte von Cloud Discovery anzuzeigen.
- Für den ausgewählten Cloud-Dienst den Zugriff blockieren oder erlauben.

Diese Blockierfunktion ist nur verfügbar, wenn Sie Kaspersky Next Expert View unter einer Lizenz für Kaspersky Next EDR Optimum oder 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.

Aktive Bedrohungen

Informationen über unverarbeitete Dateien, die sich auf den Client-Geräten befinden, finden Sie im Abschnitt **Datenverwaltung** im Unterabschnitt **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. Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Aktive Bedrohungen**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen neben der Datei, die Sie desinfizieren müssen.
   - Klicken Sie auf den Namen der Datei, die Sie desinfizieren müssen.
3. Starten Sie die Desinfektion der Datei, indem Sie auf die Schaltfläche **Desinfizieren** klicken.

   Anschließend wird versucht, die ausgewählte 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 Abschnitt **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 Abschnitt **Aktive Bedrohungen** gelöscht.

Die Möglichkeiten zur Desinfektion und Löschung von Dateien können je nach installierter Sicherheitsanwendung, Version und Einstellungen variieren.

Unverarbeitete Dateien herunterladen

Kaspersky Next Expert View ermöglicht Ihnen das Herunterladen 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 dem Gerät mit installierter Kaspersky Next Expert View in den angegebenen Ordner heruntergeladen.

Sie können Kopien von Dateien herunterladen, wenn Dateien im Zuge ihrer Desinfektion gelöscht oder verändert wurden. Die Kopien dieser Dateien werden auf dem verwalteten Gerät im Speicher von Kaspersky Endpoint Security für Linux abgelegt.

So laden Sie die Kopie einer unverarbeiteten Datei herunter:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Aktive Bedrohungen**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen neben der Datei, die Sie herunterladen müssen.
   - Klicken Sie auf den Namen der Datei, die Sie herunterladen müssen.
3. Um den Download zu starten, klicken Sie auf die Schaltfläche **Herunterladen**.

Daraufhin lädt die Sicherheitsanwendung des Client-Geräts, auf dem die ausgewählte unverarbeitete Datei gefunden wurde, eine Kopie der Datei in den angegebenen Ordner herunter.

Dateien aus dem Abschnitt "Aktive Bedrohungen" löschen

*So löschen Sie Dateien aus dem Abschnitt **Aktive Bedrohungen**:*

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Aktive Bedrohungen**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen neben der Datei, die Sie löschen müssen.
   - Klicken Sie auf den Namen der Datei, die Sie löschen müssen.
3. Löschen Sie die Dateien, indem Sie auf die Schaltfläche **Löschen** klicken.
4. Klicken Sie in dem folgenden Fenster auf die Schaltfläche **Löschen**.

   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 Abschnitt **Aktive Bedrohungen** gelöscht.

Arbeiten mit Kaspersky Next Expert View unter der Lizenz für Kaspersky Next XDR Optimum

Wenn Sie eine Lizenz für Kaspersky Next XDR Optimum als Teil einer EPP-Anwendungslizenz und einer Lizenz für Kaspersky Next Expert View erworben haben, können Sie die Funktionalität von Kaspersky Next XDR Optimum nach der Erstkonfiguration nutzen.

Wenn Sie nach der Installation und Aktivierung von Kaspersky-Anwendungen auf Geräten eine Lizenz für Kaspersky Next XDR Optimum separat als Erweiterung einer zuvor erworbenen Lizenz erworben haben, müssen Sie je nachdem, wie Sie die Lizenz für Kaspersky Next XDR Optimum erworben haben, Kaspersky Next Expert View auf den Geräten mithilfe des neuen Aktivierungscodes oder der Schlüsseldatei reaktivieren. Anschließend können Sie die Erstkonfiguration durchführen.

Nachdem Sie den Administrationsserver unter Ihrer Lizenz für Kaspersky Next XDR Optimum aktiviert und Ihren verwalteten Anwendungen den Lizenzschlüssel bereitgestellt haben, können Sie Folgendes tun:

- Reagieren Sie auf Bedrohungen, indem Sie Integrationen mit Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox und Active Directory vornehmen.
- Alarme nach Attributen gruppieren.

Weitere Informationen zu den Funktionen, die durch die Lizenz für Kaspersky Next XDR Optimum aktiviert werden, finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Darüber hinaus können Sie die Funktionen von Kaspersky Next XDR Optimum im Test-Modus nutzen. Dazu müssen Sie einen Testarbeitsbereich erstellen und anschließend Ihren verwalteten Anwendungen den Test-Lizenzschlüssel bereitstellen. Die Funktionen von Kaspersky Next XDR Optimum stehen bis zum Ablauf Ihres Testarbeitsbereichs zur Verfügung.

Integrationen für die Reaktion auf Alarme

Für die folgenden Lösungen können Sie Integrationen konfigurieren, um auf Bedrohungen zu reagieren:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Um Integrationen zu konfigurieren, müssen die folgenden Bedingungen erfüllt sein:

- Wenn Sie die Funktionen von Kaspersky Next XDR Optimum im kommerziellen Modus verwenden möchten, müssen Sie:
  - Über einen kommerziellen Arbeitsbereich und die Berechtigungen **Lesen** und **Schreiben** für den Funktionsbereich **Allgemeine Funktionen: Anwendungsintegration** verfügen.
  - Den Administrationsserver unter einer Lizenz von Kaspersky Next XDR Optimum aktivieren.
  - Ihren verwalteten Anwendungen den Lizenzschlüssel von Kaspersky Next XDR Optimum bereitstellen, um Reaktionsmaßnahmen durchzuführen.

  Wenn Sie die Lizenz für Kaspersky Next EDR Optimum verwenden, müssen Sie die Anwendungen, die auf Ihren verwalteten Geräten installiert sind, nicht unter der Lizenz für Kaspersky Next XDR Optimum aktivieren. Sie müssen dies nur für neue Geräte tun (falls vorhanden).
  Da die Lizenz von Kaspersky Next XDR Optimum Mehrmandantenfähigkeit unterstützt, können Sie den Lizenzschlüssel zentral an verwaltete Anwendungen verteilen. Die automatische Verteilung des Lizenzschlüssels auf sekundäre und virtuelle Administrationsserver wird nicht unterstützt.

- Wenn Sie die Funktionen von Kaspersky Next XDR Optimum im Testmodus verwenden möchten, müssen Sie einen Testarbeitsbereich erstellen und anschließend Ihren verwalteten Anwendungen den Demolizenz-Schlüssel bereitstellen. Die Funktionen von Kaspersky Next XDR Optimum stehen bis zum Ablauf Ihres Testarbeitsbereichs zur Verfügung.

Integration mit Active Directory für die Ausführung von Reaktionsmaßnahmen konfigurieren

Die Integration mit Active Directory ermöglicht es Ihnen, Reaktionsmaßnahmen für Active Directory-Benutzer auszuführen, die vom Alarm betroffen oder daran beteiligt sind.

Die Integration mit Active Directory für die Reaktion auf Alarme, die ADFS-Integration und die Einstellungen für die Untersuchung des Active Directory-Domänencontrollers (Adresse und Anmeldeinformationen des Domänencontrollers), die Sie bei der Konfiguration der Abfrage des Domänencontrollers angeben, sind unterschiedliche Einstellungen. Da Sie sicherstellen müssen, dass der Benutzer, für den eine Reaktionsmaßnahme ausgeführt werden soll, über ein Active Directory-Konto verfügt, müssen Sie beide Integrationen konfigurieren: für die Untersuchung und für die Reaktion. Die Reihenfolge spielt dabei keine Rolle.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Gehen Sie wie folgt vor, um die Integration mit Active Directory für die Reaktion auf Alarme zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wählen Sie den Abschnitt **Verteilungspunkte** aus und klicken Sie dann auf den Namen des gewünschten Verteilungspunkts.

3. Wählen Sie im sich öffnenden Eigenschaftenfenster den Abschnitt „**Verbindungs-Gateway**“ aus und aktivieren Sie anschließend die Option „**Verbindungs-Gateway**“.

4. Wählen Sie den Abschnitt **Active Directory** aus.

5. Aktivieren Sie im rechten Bereich den Umschalter **Integration von Active Directory**.

   Wenn Sie die Integration später deaktivieren möchten, können Sie dies nur für alle Verbindungen tun, indem Sie den Umschalter **Integration von Active Directory** deaktivieren. Sie können die Integration nicht für eine einzelne Verbindung deaktivieren. Stattdessen können Sie die Verbindung löschen.

6. Stellen Sie eine Verbindung zum Active Directory-Domänencontroller her, indem Sie auf die Schaltfläche **Verbindung hinzufügen** klicken.

7. Passen Sie im nächsten Fenster die folgenden Parameter für die Verbindung an:

   - **Adresse des Domänencontrollers**

     Name des Computers, z. B. `server.example.com`.

     Sie können mehrere Adressen angeben. Alle Domänencontroller, deren Adressen Sie angeben, müssen zu derselben Domäne gehören.

   - **Active Directory-Domänenname**

     Vollständig qualifizierter DNS-Domänenname, z. B. `example.com`

     Sie können auch den SAM- oder NetBIOS-Namen angeben, z. B. `example`

     Verwenden Sie Kleinbuchstaben. Wenn Sie mehrere Verbindungen für den Administrationsserver oder einen Verteilungspunkt erstellen, geben Sie für jede Verbindung einen anderen Namen an.

     > Mi empfiehlt nicht, die Adresse eines bestimmten Domänencontrollers und einen kurzen Domänennamen (SAM oder NetBIOS) zu verwenden.
     > Um Reaktionsmaßnahmen durchzuführen, muss der in diesem Feld angegebene Active Directory-Domänenname mit dem im Alarm angegebenen Active Directory-Domänennamen übereinstimmen.

   - **Anmelden**

     Benutzername des Active Directory-Kontos mit Administratorrechten, unter dem die Reaktionsmaßnahmen ausgeführt werden sollen.

   - **Kennwort**

     Kennwort des Active Directory-Kontos mit Administratorrechten, unter dem die Reaktionsmaßnahmen ausgeführt werden sollen.

8. Wenn Sie den Verbindungsstatus überprüfen möchten, klicken Sie auf die Schaltfläche **Verbindung prüfen**.

   Wenn die Verbindung erfolgreich hergestellt wurde, wird der Status **Verbunden** angezeigt. Andernfalls lautet der Status **Fehlgeschlagen** und es wird eine Fehlermeldung für die Domänencontroller angezeigt, zu denen Sie keine Verbindung herstellen konnten.

   > Sie müssen berücksichtigen, wie Sie eine Verbindung mit Active Directory herstellen: **von einem Linux-Gerät oder von einem Windows-Gerät**.

Verbindung von einem Linux-Gerät herstellen

Wenn Sie sich von einem Linux-Gerät aus mit einem Domänencontroller verbinden und sich bei ihm authentifizieren, sieht die Logik standardmäßig wie folgt aus:

1. Ein Verteilungspunkt versucht, über LDAPS eine Verbindung mit dem Domänencontroller herzustellen.

   Es wird eine strenge Überprüfung des LDAP-Serverzertifikats durchgeführt.

2. Um das Zertifikat zu validieren, legen Sie den öffentlichen Teil des Domänencontroller-Zertifikats im Zertifikatsspeicher des Systems ab.

   Für den Zugriff auf die Zertifikatskette wird der vom Betriebssystem abhängige Pfad zur Zertifizierungsstelle (CA) des Systems verwendet.

   Beispielsweise:

   - /etc/ssl/certs/ca-certificates.crt – Pfad für Debian-basierte Betriebssysteme (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem – Pfad für CentOS oder Red Hat.

3. Wenn die LDAP-Verbindung fehlschlägt, tritt ein Fehler auf und es wird kein anderes Verbindungsprotokoll verwendet.

> Bei Problemen mit LDAP können Sie sich an den Technischen Support von Kaspersky wenden.

Wenn Sie das Zertifikat nicht im Zertifikatsspeicher des Systems installieren möchten, können Sie das Flag KLNAG_LDAP_SSL_CACERT verwenden, um den Pfad zum Domänencontroller-Zertifikat festzulegen. Führen Sie dazu folgenden Befehl aus:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

wobei `</path/to/domain-controller/cert>` der Pfad zum öffentlichen Teil des Domänencontroller-Zertifikats ist.

Wenn der Pfad beispielsweise `"/var/opt/kaspersky/ldap_cert.crt"` lautet, lautet der Befehl `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Verbindung von einem Windows-Gerät herstellen

Wenn Sie sich von einem Windows-Gerät aus mit einem Domänencontroller verbinden und sich bei diesem authentifizieren, werden die Verbindungseinstellungen von der Domäne festgelegt.

Sie müssen nur Folgendes sicherstellen:

- LDAPS ist aktiviert und Port 636 ist auf dem Gerät verfügbar.
- Sie erlauben Verbindungen zum Domänencontroller durch eine Firewall oder einen Proxyserver.

9. Klicken Sie auf die Schaltfläche **Erstellen**.

   Das Fenster wird geschlossen und die Verbindung wird in der Verbindungstabelle angezeigt.

In der Verbindungstabelle sind folgende Aktionen möglich:

- Verbindungsparameter bearbeiten.

  Klicken Sie dazu für die gewünschte Verbindung auf den Link mit dem Parameter **Adresse des Domänencontrollers**. Ändern Sie im neuen Fenster die gewünschten Einstellungen und klicken Sie anschließend auf die Schaltfläche **Speichern**.

  Sie können nur die Parameter **Anmelden** und **Kennwort** bearbeiten.

- Verbindungen löschen.

  Aktivieren Sie dazu das Kontrollkästchen neben der Verbindung, die Sie löschen möchten, klicken Sie auf die Schaltfläche **Entfernen** in der Werkzeugleiste und bestätigen Sie anschließend das Löschen der Verbindung.

Integration mit der Kaspersky Automated Security Awareness Platform konfigurieren

Die Integration in die Kaspersky Automated Security Awareness Platform (im Folgenden auch KASAP genannt) ermöglicht die Zuordnung von KASAP-Lernkursen für Benutzer, die mit Alarmen verknüpft sind.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Bevor Sie eine Integration in Kaspersky Next Expert View konfigurieren können, müssen Sie einen Autorisierungs-Token erstellen und eine URL für API-Anfragen in KASAP anfordern.

Gehen Sie wie folgt vor, um die Integration mit der Kaspersky Automated Security Awareness Platform zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wählen Sie im Abschnitt **Integrationen** die Option **KASAP** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **KASAP-Integration**.

4. Geben Sie die Einstellungen an, die für die Verbindung mit KASAP verwendet werden sollen:

   - **API-Token**: Token, das Sie für den Zugriff auf die Open API von KASAP erstellt haben.

   - **URL**: URL für API-Anfragen, die Sie beim Erstellen des API-Tokens erhalten haben.

5. Überprüfen Sie gegebenenfalls Ihre Einstellungen, indem Sie auf die Schaltfläche **Verbindung prüfen** klicken.

   Der Verbindungsstatus wird angezeigt.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Integration mit der Kaspersky Automated Security Awareness Platform ist konfiguriert.

Nachdem die Einstellungen der KASAP-Integration gespeichert wurden, können Sie die Liste der KASAP-Lerngruppen anzeigen, indem Sie auf die Schaltfläche **Gruppen anzeigen** klicken.

Wenn die Gruppenliste angezeigt wird, können Sie sie bei Bedarf aktualisieren, indem Sie auf die Schaltfläche **Gruppen aktualisieren** klicken.

Die Liste kann nach dem Öffnen nicht ausgeblendet werden. Wenn Sie den Umschalter für die **KASAP-Integration** deaktivieren, wird die Liste der KASAP-Gruppen nicht angezeigt.

Integration mit Kaspersky Threat Intelligence Portal Sandbox konfigurieren

Die Integration mit Kaspersky Threat Intelligence Portal (im Folgenden auch Kaspersky TIP genannt) ermöglicht die Ausführung der Dateien, die mithilfe von Kaspersky Sandbox in die **Quarantäne** verschoben wurden – eine sichere Umgebung, die von Ihrem Unternehmensnetzwerk isoliert ist.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Bevor Sie die Integration konfigurieren, müssen Sie ein Autorisierungs-Token für API-Anfragen auf Kaspersky TIP anfordern.

Gehen Sie wie folgt vor, um die Integration mit Kaspersky TIP Sandbox zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wählen Sie **Kaspersky TIP** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **Integration**.

   Die Einstellungen für die Verbindung mit Kaspersky TIP werden angezeigt.

   Wenn Sie nach dem Konfigurieren und Speichern der Integrationseinstellungen den Umschalter **Integration** deaktivieren, werden die Einstellungen nicht gelöscht, aber Sie können die Reaktionsmaßnahme nicht ausführen.

4. Klicken Sie auf die Schaltfläche **Token hinzufügen**, geben Sie im angezeigten Fenster das Token an, das Sie zuvor über Kaspersky TIP erhalten haben, und klicken Sie dann auf die Schaltfläche **Hinzufügen**.

   Das Fenster wird geschlossen und das API-Token wird hinzugefügt.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Integration mit Kaspersky TIP Sandbox ist konfiguriert.

Jetzt können Sie Dateien aus der **Quarantäne** zur Bedrohungsanalyse an Kaspersky TIP Sandbox senden. Die maximale Größe einer Datei beträgt 100 MB.

Da die Lizenz für Kaspersky Next XDR Optimum die Mandantenfähigkeit unterstützt, können Dateien, die in die **Quarantäne** verschoben werden, nach Mandanten aufgeteilt werden. Diese Trennung auf Mandantenebene kann auch für das Senden von Dateien an Kaspersky TIP Sandbox und die Anzeige der Ergebnisse angewendet werden, wenn der Administrator ein dediziertes TIP-Konto und ein API-Token für jeden Mandanten verwendet. Eine zentrale Verwaltung des Abschnitts **Quarantäne** für alle Mandanten ist jedoch nicht möglich, da die Quarantäneliste Objekte nicht entsprechend der Serverhierarchie anzeigt.

Alarme nach Attributen gruppieren

Um die Funktion zum Aggregieren von Alarmen im kommerziellen Modus zu aktivieren, müssen Sie den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum aktivieren und anschließend den Lizenzschlüssel für Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereitstellen. Wenn Sie die Lizenz für Kaspersky Next EDR Optimum verwenden, müssen Sie die Anwendungen, die auf Ihren verwalteten Geräten installiert sind, nicht unter der Lizenz für Kaspersky Next XDR Optimum aktivieren. Sie müssen dies nur für neue Geräte tun (falls vorhanden).
Da die Lizenz für Kaspersky Next XDR Optimum Mehrmandantenfähigkeit unterstützt, können Sie den Lizenzschlüssel zentral an verwaltete Anwendungen verteilen. Die automatische Verteilung der Lizenz auf sekundäre und virtuelle Administrationsserver wird nicht unterstützt.

Im Testmodus müssen Sie über einen Testarbeitsbereich verfügen und Ihren verwalteten Anwendungen den Demolizenz-Schlüssel bereitstellen. Die Funktion zur Aggregation von Alarmen ist bis zum Ablauf Ihres Testarbeitsbereichs verfügbar.

Die Aggregation gruppiert Alarme, die möglicherweise zum selben Vorfall gehören, was den Untersuchungsprozess vereinfacht. Sie können Alarme nach Gerätename, Konto oder Hash-Name (SHA256) aggregieren.

Alarme werden nur dann nach einem Attribut aggregiert, wenn dieses Attribut nicht leer ist.

Alarme werden aggregiert, wenn sie mindestens ein Attribut gemeinsam haben und innerhalb von 24 Stunden nach einem anderen Alarm in der Gruppe auftreten.

Gehen Sie wie folgt vor, um Alarme nach Attributen zu aggregieren:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Alarme**.

2. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie den Umschalter **Aggregation von Alarmen** und wählen Sie dann ein oder mehrere Attribute aus, nach denen Alarme aggregiert werden sollen:

     - **Gerätename**
     - **Benutzerkonto**
     - **Datei-Hash (SHA256)**

     Die Attribute **Gerätename** und **Benutzerkonto** sind standardmäßig ausgewählt.

   - Klicken Sie auf das Einstellungen-Symbol (). Gehen Sie im nächsten Fenster „**Tabelleneinstellungen**“ zur Registerkarte „**Gruppierung**“. Wählen Sie **ID der Aggregationsgruppe** aus und klicken Sie auf **Übernehmen**.

   Wenn das Aggregieren aktiviert ist, werden die Alarme nach **Ereigniszeitpunkt** vom neuesten zum ältesten sortiert. Zusätzliche Sortieroptionen werden nicht unterstützt. Wenn Sie eine andere Optionsgruppe auswählen, wird das Aggregieren deaktiviert.

In der Tabelle werden die nach Attributen aggregierten Alarme angezeigt. Nicht aggregierte Alarme werden unten in der Tabelle angezeigt.

Jeder Alarm wird nach dem Aggregieren nur einer Gruppe zugewiesen.

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, gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (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 auf der Registerkarte **Erweitert** 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 **Kaspersky-Anwendungen** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.
3. Wählen Sie in der Programmliste 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 Kaspersky Security-Agenten 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 **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 **Kaspersky-Anwendungen** 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 **Stufe der Xperf-Ablaufverfolgung 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:

- **Basic**

  Die Ablaufverfolgungsinformationen werden während der Ausführung der Sicherheitsanwendung Kaspersky Endpoint Security empfangen.

  Diese Variante ist standardmäßig ausgewählt.

- **Bei Neustart**

  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

Sie können Protokolldatei von einem Client-Gerät nur dann herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird ein Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

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 **Kaspersky-Anwendungen** 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.

   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

Sie können die Programmeinstellungen von einem Client-Gerät nur dann herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird ein Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

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 **Kaspersky-Anwendungen** aus.
3. Klicken Sie im Abschnitt **Anwendungseinstellungen** 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.

Systeminformationen von einem Client-Gerät herunterladen

Sie können die Systeminformationen von einem Client-Gerät nur dann auf Ihr eigenes Gerät herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird ein Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

So laden Sie Systeminformationen von einem Client-Gerät herunter:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Systeminformationen** aus.
3. Klicken Sie auf die Schaltfläche **Herunterladen**, um die Systeminformationen über das Client-Gerät herunterzuladen.

Die Datei mit den Informationen wird an den angegebenen Speicherort heruntergeladen.

Ereignisprotokolle downloaden

Sie können die Ereignisprotokolle von Client-Gerät nur dann herunterladen, wenn eine der folgenden Bedingungen erfüllt ist: Die Option **Verbindung mit Administrationsserver nicht trennen** ist in den Geräteeinstellungen aktiviert, es wird Push-Server verwendet oder es wird ein Verbindungs-Gateway verwendet. Andernfalls ist der Download nicht möglich.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

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.
     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 **Kaspersky-Anwendungen** 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:
   - **Anwendung beenden**
     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Anwendung neu starten**
     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.

- **Anwendung 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.

Ausführen der Ferndiagnose eines Programms und Herunterladen der Ergebnisse

Um die Diagnose für ein Programm auf einem Remote-Gerät zu starten und die Ergebnisse 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 **Kaspersky-Anwendungen** 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 Ferndiagnose ausführen möchten.

   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 Supportspezialist von Kaspersky Sie dazu auffordert. Sie müssen das Programm nicht auf dem Gerät installieren.

Wenn Sie auf dem Client-Gerät ein benutzerdefiniertes Skript ausführen möchten, können Sie die Umgebungsvariable `KLACDT_SAVE_SETTING` verwenden, um den Pfad zum Speichern der Ausführungsergebnisse zu bestimmen. Beispielsweise:

- Für ein Gerät auf Windows-Basis:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Für ein Gerät auf Linux-Basis:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

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. Wählen Sie im Feld **Objekttyp** den Objekt-Typ des Objekts, das Sie hochladen möchten:
   - Wählen Sie **Datei**, um die ausführbare Datei hochzuladen.
   - Wählen Sie **Ordner**, um den Ordner mit der Anwendung hochzuladen, die Sie auf dem Client-Gerät ausführen möchten.

     Wenn Sie diesen Objekt-Typ auswählen, wird das Feld **Name der zu startenden ausführbaren Datei** angezeigt. Geben Sie in diesem Feld den Namen der ausführbaren Datei im Ordner an. Sie können auch den relativen Pfad zu der Datei angeben.
   - Wählen Sie **Archiv**, um das zip-Archiv mit der Anwendung hochzuladen, die Sie auf dem Client-Gerät ausführen möchten.

     Wenn Sie diesen Objekt-Typ auswählen, wird das Feld **Name der zu startenden ausführbaren Datei** angezeigt. Geben Sie in diesem Feld den Namen der ausführbaren Datei im Ordner an, die Sie auf dem Client-Gerät ausführen möchten. Sie können auch den relativen Pfad zu der Datei angeben.

     > 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.
4. Laden Sie das Objekt hoch, indem Sie es im Standard-Dialog des Betriebssystems auswählen oder in das Upload-Feld ziehen.
5. Geben Sie bei Bedarf im Feld **Kommandozeilenargumente** die Befehlszeilenargumente an, die beim Ausführen der ausführbaren Datei übergeben werden sollen.
6. Klicken Sie auf die Schaltfläche **Hochladen und ausführen**, um die angegebene Anwendung auf einem Client-Gerät auszuführen.
7. Nachdem die Anwendung erfolgreich ausgeführt wurde, laden Sie die Ausführungsergebnisse herunter, indem Sie auf die Schaltfläche **Ausführungsergebnisse der Anwendung herunterladen** klicken.

   > Die Ergebnisse einer Anwendungsausführung werden so lange gespeichert, bis Sie eine erneute Diagnose ausführen oder das Fenster schließen.

Die Ferndiagnose eines Client-Geräts mithilfe der Anwendung ist abgeschlossen.

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 Generieren von Dump-Dateien ist nur für 32-Bit-Prozesse verfügbar, die auf Windows-basierten Client-Geräten ausgeführt werden. Diese Funktion wird für Linux-Client-Geräte und 64-Bit-Prozesse nicht unterstützt.

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 Ferndiagnose-Fenster 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 **Herunterladen**, um die Dump-Datei für die angegebene Anwendung zu speichern.

   Wenn die angegebene Anwendung nicht auf dem Client-Gerät ausgeführt wird, erscheint eine Fehlermeldung.

Ferndiagnose auf einem Linux-basierten Client-Gerät ausführen

Kaspersky Next Expert View 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 Next Expert View 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.

Ereignisse in SIEM-Systeme exportieren

Dieser Abschnitt beschreibt, wie Sie den Export von Ereignissen in ein SIEM-System konfigurieren.

Ereignisexport in SIEM-Systeme konfigurieren

Dieser Abschnitt enthält ein Szenario zum Konfigurieren des Exports von Ereignissen vom Administrationsserver in externe SIEM-Systeme. 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 den Gruppen der Geräte auftreten, operativ zu reagieren.

Erforderliche Vorrausetzungen

Bevor Sie mit der Konfiguration des Ereignisexports in die Kaspersky Next Expert View 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.

Schritte

Der Prozess des Ereignisexports in SIEM-Systeme umfasst die folgenden Schritte:

- **Konfigurieren des SIEM-Systems, so dass es Ereignisse aus Kaspersky Next Expert View empfängt**

  Sie müssen im SIEM-System das Empfangen von Ereignissen von Kaspersky Next Expert View konfigurieren.

- **Markieren von Ereignissen für den Export**

  Sie müssen markieren, welche Ereignisse Sie in das SIEM-System exportieren möchten. Markieren Sie als Erstes die allgemeinen Ereignisse die in allen verwalteten Kaspersky-Anwendungen auftreten. Darüber hinaus können Sie Ereignisse für bestimmte verwaltete Kaspersky-Anwendungen markieren.

- **Konfiguration von Kaspersky Next Expert View für den Export an ein SIEM-System**

  Sie müssen Kaspersky Next Expert View konfigurieren, um den Export von Ereignissen an ein SIEM-System zu beginnen.

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 die Kaspersky Next Expert View müssen einige Einstellungen des SIEM-Systems angegeben werden. Es ist empfehlenswert, diese Einstellungen im Voraus zu bestimmen, damit die Einstellungen für Kaspersky Next Expert View 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 Next Expert View und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Next Expert View und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

- **Protokoll**

  Das Protokoll, das für die Übertragung von Daten aus Kaspersky Next Expert View ins SIEM-System verwendet wird. Dieser Wert muss in den Einstellungen von Kaspersky Next Expert View und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

Über den Ereignisexport

Kaspersky Next Expert View 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 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 Next Expert View in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Next Expert View – und der Empfänger der Ereignisse – ein SIEM-System. Für einen erfolgreichen Ereignisexport müssen die Einstellungen sowohl im verwendeten SIEM-System als auch in der Kaspersky Next Expert View angepasst werden. Die Reihenfolge der Einstellungen hat keine Bedeutung: Sie können entweder zuerst den Versand der Ereignisse in der Kaspersky Next Expert View und dann das Empfangen der Ereignisse im SIEM-System anpassen, oder umgekehrt.

Syslog-Format des Ereignisexports

Sie können Ereignisse im Syslog-Format an ein beliebiges SIEM-System senden. Mit dem Syslog-Format können beliebige Ereignisse übertragen werden, die auf dem Administrationsserver und in Kaspersky-Anwendungen, auf verwalteten Geräten installiert sind, auftreten. Beim Exportieren von Ereignissen im Syslog-Format können Sie genau festlegen, welche Arten von Ereignissen an das SIEM-System übertragen werden.

Empfangen von Ereignissen im SIEM-System

Das SIEM-System muss die von Kaspersky Next Expert View 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.

Den Ereignisexport in ein SIEM-System konfigurieren

Am Ablauf des Ereignisexports aus Kaspersky Next Expert View in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Next Expert View – und der Empfänger der Ereignisse – ein SIEM-System. Der Ereignisexport wird im verwendeten SIEM-System und in der Kaspersky Next Expert View 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 Next Expert View gesendet werden, angepasst werden. Im Allgemeinen müssen im SIEM-System die folgenden Einstellungen angegeben werden:

- **Port**

  Geben Sie die Portnummer für die Verbindung mit Kaspersky Next Expert View an. Es muss derselbe Port angegeben werden, den Sie als Port in Kaspersky Next Expert View während der Konfiguration mit einem SIEM-System festlegen.

- **Übertragungsprotokoll der Nachrichten oder Typ der Quelldaten**

  Geben Sie das Syslog-Format an.

Je nach verwendetem SIEM-System kann erforderlich sein, erweiterte Einstellungen für den Empfänger der Nachrichten anzugeben.

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. Der Nachrichtenparser ist im SIEM-System integriert – er wird für die Aufteilung der Nachrichten in Felder, etwa Ereignis-ID, Signifikanz, Beschreibung und die übrigen Einstellungen verwendet. Daraufhin hat das SIEM-System die Möglichkeit, die Ereignisse, die aus Kaspersky Next Expert View 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 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 **Asset-Verwaltung** → **Richtlinien**.
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 **Asset-Verwaltung** → **Assets (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 **Anwendungen**.
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 auf den Namen des Administrationsservers.
   - Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien** → 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 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 Next Expert View in externe Systeme verwendet.

In Kaspersky Next Expert View 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 Next Expert View so angepasst, dass der Versand von Ereignissen ins SIEM-System ausgeführt werden kann. Der Versand von Ereignissen aus Kaspersky Next Expert View 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 Next Expert View für den Export an ein SIEM-System

Um Ereignisse an ein SIEM-System zu exportieren müssen Sie den Exportprozess in Kaspersky Next Expert View konfigurieren.

So konfigurieren Sie den Export in SIEM-Systeme in Kaspersky Next Expert View:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wechseln Sie zum Abschnitt **SIEM** und klicken Sie anschließend auf den Link **Einstellungen**.

3. Im neuen rechten Bereich können Sie die **Export-Einstellungen angeben**.

   - Geben Sie im Feld **Serveradresse des SIEM-Systems** die IP-Adresse des Servers an, auf dem das aktuell verwendete SIEM-System installiert ist.

     Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

   - Geben Sie im Feld **Port des SIEM-Systems** die Portnummer an, die zur Herstellung der Verbindung zwischen Kaspersky Next Expert View und Ihrem SIEM-System verwendet wird.

     Dieser Wert muss in den Einstellungen von Kaspersky Next Expert View und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

   - Der Wert in der Liste **Protokoll** ist vorausgewählt. Zum Übertragen von Nachrichten an das SIEM-System können Sie ausschließlich das "TLS over TCP"-Protokoll verwenden.

- Wählen Sie in der Dropdown-Liste **Authentifizierung des Servers** einen der folgenden Einträge:

  - **Vertrauenswürdige Zertifikate**. Klicken Sie anschließend auf die angezeigte Schaltfläche **CA-Zertifikatsdatei auswählen**, um das vertrauenswürdige Zertifikat hochzuladen.

    Sie können eine vollständige Zertifikatkette (einschließlich des Root-Zertifikats) von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority – CA) abrufen und diese Datei in Kaspersky Next Expert View hochladen. Kaspersky Next Expert View prüft, ob die Zertifikatkette des SIEM-Servers auch von einer vertrauenswürdigen CA signiert ist oder nicht.

  - **SHA-Fingerabdrücke**. Geben Sie anschließend im Feld **Fingerabdrücke** den SHA1-Fingerabdruck ein und klicken Sie auf die Schaltfläche **Hinzufügen**.

    Sie können SHA1-Fingerabdrücke der vollständigen Zertifikatkette des SIEM-Systems (einschließlich des Root-Zertifikats) in Kaspersky Next Expert View angeben.

- Klicken Sie auf den Link **Namen/Alternativen Namen des Antragstellers hinzufügen**.

  Der Link wird nur angezeigt, wenn Sie in der Dropdown-Liste **Authentifizierung des Servers** den Eintrag **Vertrauenswürdige Zertifikate** ausgewählt haben.

  Der Antragstellername ist ein Domänenname, für den das Zertifikat empfangen wird. Kaspersky Next Expert View 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/Alternativer Name des Antragstellers** angeben. Wenn einer der angegebenen Antragstellernamen mit dem Antragsteller des Zertifikats für das SIEM-Systems übereinstimmt, validiert Kaspersky Next Expert View das Zertifikat dieses SIEM-Systems.

- Klicken Sie auf den Link **Client-Authentifizierung hinzufügen** und wählen Sie anschließend in der Dropdown-Liste **Wenn Sie kein Zertifikat besitzen, können Sie eines generieren** einen der folgenden Einträge aus:

  - **Schlüssel generieren**. Klicken Sie anschließend auf die Schaltfläche **Generieren**, wenn Sie in Kaspersky Next Expert View ein selbstsigniertes Zertifikat generieren möchten. Infolge dessen speichert Kaspersky Next Expert View das generierte selbstsignierte Zertifikat und Sie können den öffentlichen Teil des Zertifikats oder den SHA1-Fingerabdruck an das SIEM-System übergeben.

    Durch die Verwendung der Einstellung können Sie ein Zertifikat generieren, um Kaspersky Next Expert View zu authentifizieren. Infolge dessen verwenden Sie ein selbstsigniertes Zertifikat, das von Kaspersky Next Expert View ausgestellt wurde. In diesem Fall können Sie sowohl ein vertrauenswürdiges Zertifikat als auch einen SHA-Fingerabdruck verwenden, um den SIEM-Systemserver zu authentifizieren.

  - **Zertifikat einfügen**, wenn Sie ein Zertifikat verwenden möchten, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen CA.

    Geben Sie anschließend das Zertifikat und dessen privaten Schlüssel wie folgt an:

    a. Wählen Sie in der Dropdown-Liste **Client-Zertifizierung** den Zertifikatstyp aus:

    - **X.509-Zertifikat im PEM-Format**
    - **X.509-Zertifikat im PKCS12-Format**

b. Laden Sie im Feld **Datei mit Zertifikat** die Datei mit dem Zertifikat hoch.

c. Wenn Sie **X.509-Zertifikat im PEM-Format** ausgewählt haben, laden Sie im angezeigten Abschnitt **Datei mit Schlüssel** die Datei mit dem privaten Schlüssel hoch.

Die Datei mit dem Zertifikat und die Datei mit dem privaten Schlüssel sind nicht voneinander abhängig und die Dateien können in beliebiger Reihenfolge hochgeladen werden.

d. Wenn der private Schlüssel verschlüsselt ist, geben Sie im Feld **Überprüfung von Kennwort oder Zertifikat** das Kennwort zum Entschlüsseln an. Andernfalls können Sie das Feld leer lassen.

- Im Abschnitt **Datumsformat** ist der Wert **System-Protokoll** vorausgewählt.

  Die Länge einer Nachricht, die an das SIEM gesendet wird, können Sie nur im Feld **Maximale Größe der Nachricht in Byte** begrenzen. Wenn dieser Grenzwert überschritten wird, wird die Nachricht abgeschnitten.

4. Wenn Sie möchten, können Sie archivierte Ereignisse aus der Datenbank des Administrationsservers 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 im sich öffnenden Abschnitt das Startdatum im Feld **Exportieren ab dem Startdatum** an.

   c. Klicken Sie auf die Schaltfläche **OK**.

5. Setzen Sie die Option auf die Position **Ereignisse automatisch in die Datenbank des SIEM-Systems exportieren**.

6. Um zu überprüfen, ob die Verbindung mit dem SIEM-System konfiguriert wurde, klicken Sie auf die Schaltfläche **Verbindung prüfen**.

   Der Verbindungsstatus wird angezeigt.

7. Klicken Sie auf die Schaltfläche **Speichern**.

Der Export in ein SIEM-System ist konfiguriert. Wenn Sie das Empfangen von Ereignissen in einem SIEM-System konfiguriert haben, exportiert der Administrationsserver von nun an die markierten Ereignisse in ein SIEM-System. Wenn Sie das Startdatum des Exports angegeben haben, exportiert der Administrationsserver auch die markierten Ereignisse, die in der Administrationsserver-Datenbank ab dem angegebenen Datum gespeichert sind.

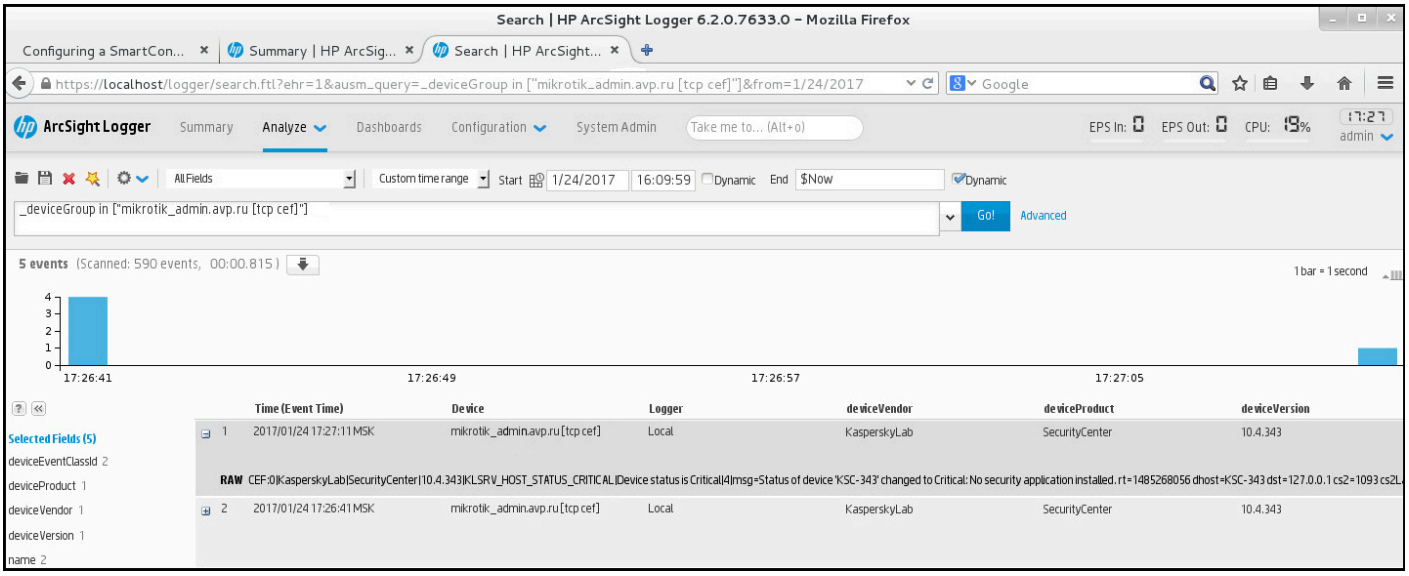
Exportergebnisse anzeigen

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 Next Expert View 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 Next Expert View 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

Schnellstartanleitung für Managed Service Provider (MSP)

Die Kurzanleitung ist für Administratoren von Managed Service Providern (MSPs) gedacht.

Die Kaspersky Next Expert View unterstützt Mandantenfähigkeit. Die Anleitung enthält Tipps und bewährte Verfahren für die Verwaltung von Kundenkonten (Mandanten) und zur Installation von Sicherheitsanwendungen auf Kundengeräten.

Über die Kaspersky Next Expert View

Kaspersky Next Expert View ist ein Programm, das von Kaspersky gehostet und verwaltet wird. Sie müssen Kaspersky Next Expert View nicht auf Ihrem Computer oder Server installieren. Mit Kaspersky Next Expert View kann der Administrator Kaspersky-Sicherheitsanwendungen auf Geräten in einem Unternehmensnetzwerk installieren, Untersuchungs- und Updateaufgaben remote ausführen und die Sicherheitsrichtlinien verwalteter Anwendungen verwalten. Der Administrator kann ein detailliertes Dashboard verwenden, das eine Momentaufnahme des Status der Unternehmensgeräte, detaillierte Berichte und spezifische Einstellungen in Schutzrichtlinien enthält.

Hauptmerkmale von Kaspersky Next Expert View

Mit Kaspersky Next Expert View können Sie Folgendes tun:

- Kaspersky-Anwendungen auf Geräten Ihres Netzwerks installieren und die installierten Anwendungen verwalten.
- Eine Hierarchie der Administrationsgruppen erstellen, um eine Gruppe von bestimmten Client-Geräten als Ganzes zu verwalten.
- Virtuelle Administrationsserver erstellen und in einer Hierarchie arrangieren.
- Ihre Netzwerkgeräte schützen, einschließlich Workstations und Server:
  - Ein auf Kaspersky-Anwendungen basierendes System für Schutz vor Malware verwalten.
  - Die Fähigkeiten von Detection and Response (EDR und MDR) nutzen (für Kaspersky Endpoint Detection and Response und/oder Kaspersky Managed Detection and Response wird eine Lizenz benötigt), einschließlich:
    - Analysieren und Untersuchen von Vorfällen
    - Visualisieren von Vorfällen durch das Erstellen eines Diagramms mit der Entwicklungskette der Bedrohung
    - Annehmen oder ablehnen von Reaktionen, sowie Aktivieren von Auto-Akzeptieren für alle Reaktionen
- Kaspersky Next Expert View als mandantenfähige Anwendung verwenden.
- Kaspersky-Anwendungen, die auf Client-Geräten installiert sind, remote verwalten.

- Die zentrale Bereitstellung von Lizenzschlüsseln für Kaspersky-Anwendungen auf Client-Geräten durchführen.
- Sicherheitsrichtlinien für Geräte in Ihrem Netzwerk erstellen und verwalten.
- Benutzerkonten erstellen und verwalten.
- Benutzerrollen erstellen und verwalten (RBAC).
- Aufgaben für Programme, die auf Ihren Netzwerkgeräten installiert sind, erstellen und verwalten.
- Für jedes Kundenunternehmen separate Berichte zum Status des jeweiligen Sicherheitssystems anzeigen.

Über die Lizenzierung der Kaspersky Next Expert View für Managed Service Provider (MSPs)

Wenn Sie Kaspersky Next Expert View starten, können Sie entweder einen Testarbeitsbereich auswählen (in diesem Fall erhalten Sie eine 30-tägige Demolizenz, die in Ihrem Arbeitsbereich eingebettet ist), oder den Aktivierungscode einer kommerziellen Lizenz eingeben.

Sie können der Datenverwaltung des Administrationsservers später noch einen oder mehrere kommerzielle Lizenzschlüssel hinzufügen.

Informationen für MSPs zu den Funktionen für Detection and Response

Kaspersky Next Expert View kann die Funktionen anderer Kaspersky-Anwendungen in der Benutzeroberfläche der Konsole integrieren. Beispielsweise können Sie Funktionalitäten für Detection and Response zu den Funktionen von Kaspersky Next Expert View hinzufügen, indem Sie die folgenden Programme integrieren:

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum ist eine Lösung zum Schutz der IT-Infrastruktur eines Unternehmens vor komplexen Cyberbedrohungen. Die Funktionalität der Lösung kombiniert die automatische Erkennung von Bedrohungen mit der Fähigkeit, auf diese Bedrohungen zu reagieren, um komplexen Angriffen zu widerstehen – einschließlich neuartiger Exploits, Ransomware, dateiloser Angriffe und Methoden, die legitime Systemtools ausnutzen.

  Wenn die Kaspersky Endpoint Protection Platform (EPP) einen Sicherheitsvorfall entdeckt, wird in der Kaspersky Next Expert View eine detaillierte Vorfallskarte mit Informationen über den Vorfall generiert. Die Vorfallskarte wird durch eine der folgenden Programme generiert:

  - Kaspersky Endpoint Agent, der zusammen mit einer EPP-Anwendung von Kaspersky installiert ist
  - Kaspersky Endpoint Security für Windows 11.7.0 oder höher, welches mit integrierten Funktionen von EDR Optimum bereitgestellt wurde und keine zusätzliche Installation von Kaspersky Endpoint Agent benötigt

  Mit einer Vorfallskarte können Sie den Vorfall analysieren und untersuchen. Außerdem können Sie den Vorfall visualisieren, indem Sie ein Diagramm zur Entwicklungskette der Bedrohung erstellen. Dieses Diagramm gibt die Phasen der Verbreitung des erkannten Angriffs in Relation zum Zeitverlauf wieder. Das erstellte Diagramm enthält Informationen über die an dem Angriff beteiligten Module und die von diesen Modulen ausgeführten Aktionen.

Sie können auch eine Reihe von Gegenreaktionen einleiten: Erstellen Sie für ein nicht vertrauenswürdiges Objekt eine Regel, die dessen Ausführung verhindert; Suchen Sie basierend auf den ausgewählten Indikatoren für eine Kompromittierung (Indicators of Compromise – IOC) nach ähnlichen Vorfällen in der Gerätegruppe; Isolieren Sie ein nicht vertrauenswürdiges Objekt; Isolieren Sie ein kompromittiertes Gerät vom Netzwerk.

Weitere Informationen zur Aktivierung des Programms finden Sie in der Dokumentation zu Kaspersky Endpoint Detection and Response Optimum.

Wenn das Programm integriert ist, wird der Abschnitt **Alarme** zur Benutzeroberfläche von Kaspersky Next Expert View hinzugefügt (**Überwachung** → **Alarme**).

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response bietet Unternehmen, die Schwierigkeiten haben, Know-how und Personal zu finden, oder die über begrenzte interne Ressourcen verfügen, rund um die Uhr Schutz vor der wachsenden Anzahl von Bedrohungen, die automatisierte Sicherheitsbarrieren umgehen. Die MDR SOC-Analysten von Kaspersky oder von einem Drittunternehmen untersuchen die Vorfälle und stellen Reaktionen zur Lösung der Vorfälle zur Verfügung. Sie können diese angebotenen Maßnahmen entweder manuell akzeptieren oder ablehnen, oder eine Option aktivieren, alle Reaktionen automatisch zu akzeptieren.

  Weitere Informationen zur Aktivierung des Programms finden Sie in der Dokumentation zu Kaspersky Managed Detection and Response.

  Wenn das Programm integriert ist, wird der Abschnitt **Vorfälle** zur Benutzeroberfläche von Kaspersky Next Expert View hinzugefügt (**Überwachung** → **Vorfälle**).

Sie können die Oberflächenelemente, die sich auf die Funktionen von Kaspersky Endpoint Detection and Response oder Kaspersky Managed Detection and Response beziehen, im Abschnitt **Einstellungen der Benutzeroberfläche** der Kaspersky Next Expert View jederzeit ein- oder ausblenden.

Erste Schritte mit Kaspersky Next Expert View

Wenn Sie das Szenario in diesem Abschnitt abgeschlossen haben, ist Kaspersky Next Expert View einsatzbereit.

Szenario: Erste Schritte

Das Szenario verläuft in den folgenden Schritten:

1. **Konto erstellen**

   Um Kaspersky Next Expert View verwenden zu können, benötigten Sie ein Konto auf Kaspersky Next Expert View.

   So legen Sie ein Benutzerkonto an:

   1. Öffnen Sie Ihren Browser und geben Sie die folgende Adresse ein: https://ksc.kaspersky.com.
   2. Klicken Sie auf die Schaltfläche **Jetzt Konto erstellen**.
   3. Folgen Sie den Anweisungen auf dem Bildschirm.

2. **Arbeitsbereich erstellen**

   Nachdem Sie das Konto erstellt haben, können Sie den ersten Arbeitsbereich erstellen. Es wird empfohlen, zunächst einen Test-Arbeitsbereich zu erstellen, Ihre eigenen Geräte mit ihm zu verbinden, und anschließend Änderungen an den Einstellungen zu testen und deren Resultate zu notieren.

Wenn Sie Kaspersky Next Expert View starten, können Sie entweder einen Testarbeitsbereich auswählen (in diesem Fall erhalten Sie eine 30-tägige Demolizenz, die in Ihrem Arbeitsbereich eingebettet ist), oder den Aktivierungscode einer kommerziellen Lizenz eingeben.

So legen Sie einen Arbeitsbereich an:

1. Öffnen Sie Ihren Browser und geben Sie die folgende Adresse ein: https://ksc.kaspersky.com.
2. Klicken Sie auf die Schaltfläche **Anmelden**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

3. **Durchführen der Erstkonfiguration von Kaspersky Next Expert View**

   Wenn Sie den erstellten Arbeitsbereich zum ersten Mal öffnen, werden Sie automatisch dazu aufgefordert, den Schnellstartassistenten auszuführen. Der Schnellstartassistent hilft Ihnen bei der Erstellung der minimal erforderlichen Aufgaben und Richtlinien, beim Anpassen einer Mindestauswahl an Einstellungen und beim Beginn der Erstellung von Installationspaketen für Kaspersky-Anwendungen. Folgen Sie den Anweisungen auf dem Bildschirm.

Wenn die Erstkonfiguration abgeschlossen wurde, ist Kaspersky Next Expert View einsatzbereit.

Empfehlungen für die Verwaltung von Kundengeräten

Dieser Abschnitt enthält Empfehlungen, wie Sie Ihre zu schützenden Kundengeräte organisieren.

Die Empfehlungen hängen dabei davon ab, ob Sie Kaspersky Security Center zum ersten Mal verwenden, oder ob Sie bereits die lokal ausgeführte Version verwendet haben:

- Wenn Sie Kaspersky Security Center noch nie eingesetzt haben, stehen Ihnen zwei Optionen zur Verfügung:
  - Erstellen Sie für die Geräte eines jeden Kunden einen virtuellen Administrationsserver (empfohlene Option). In diesem Fall können die Geräte jedes Kunden über einen separaten virtuellen Administrationsserver unabhängig von anderen Kunden verwaltet werden. Gleichzeitig können Sie mit dem primären Administrationsserver gemeinsame Richtlinien und Aufgaben für alle Kunden erstellen. Die auf dem primären Administrationsserver erstellten Berichte können Daten von allen virtuellen Administrationsservern enthalten.
  - Erstellen Sie für jeden Ihrer Kunden eine Administrationsgruppe für dessen Geräte. Wenn Sie die Kundengeräte feiner unterteilen möchten, können Sie für jede Administrationsgruppe eine Hierarchie von untergeordneten Administrationsgruppen anlegen. Sie können beispielsweise untergeordnete Gruppen gebrauchen, wenn Sie für die Geräte von Angestellten, die in verschiedenen Abteilungen arbeiten, unterschiedliche Schutzeinstellungen verwenden möchten.
- Wenn Sie bereits ein lokal ausgeführtes Kaspersky Security Center verwendet haben, können Sie Ihre bestehenden Administrationsgruppen und zugehörigen Objekte vom lokal ausgeführten Kaspersky Security Center in die Kaspersky Next Expert View migrieren.

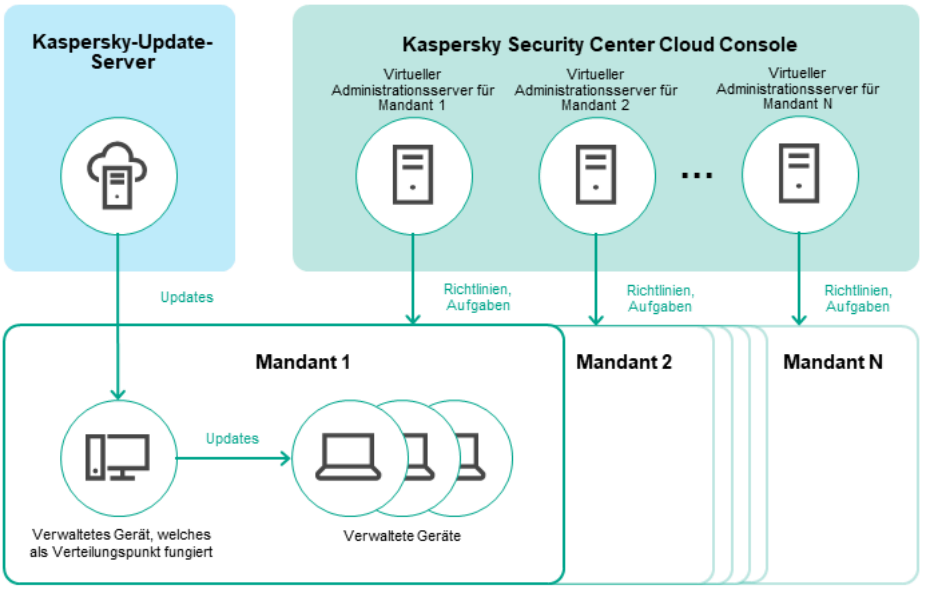
  Virtuelle Administrationsserver können nicht migriert werden. Nach der Migration der Administrationsgruppen und anderer Objekte können Sie in der Kaspersky Next Expert View virtuelle Administrationsserver erstellen.

  Fahren Sie mit der Migration fort.

Der Administrator eines virtuellen Administrationsservers kann nur ausgehend vom primären Administrationsserver zu diesem virtuellen Server wechseln. Alle auf dem primären Administrationsserver erstellten Objekte stehen dem Administrator eines virtuellen Administrationsservers zum Lesen zur Verfügung (z. B. Widgets, Berichte oder Benutzerrollen).

Typisches Bereitstellungsschema für Managed Service Provider (MSPs)

Dieser Abschnitt enthält eine Beschreibung des Bereitstellungsschemas, das normalerweise von MSPs verwendet wird, um mehrere Mandanten zu verwalten. Das Schema basiert auf der Verwaltung durch virtuelle Administrationsserver, die individuell für jeden Mandanten erstellt werden.



Typisches Bereitstellungsschema für Managed Service Provider (MSPs)

Das Schema umfasst die folgenden Hauptkomponenten:

- *Kaspersky Next Expert View*. Stellt eine Benutzeroberfläche für die Verwaltungsdienste Ihres Arbeitsbereichs zur Verfügung. Sie verwenden die Komponente von Kaspersky Next Expert View, um das Schutzsystem für das Netzwerk eines Kundenunternehmens bereitzustellen, zu verwalten und zu warten.

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

- *Virtuelle Administrationsserver*. In der Regel erstellt ein MSP-Administrator für jeden Mandanten einen virtuellen Administrationsserver, um das Schutzsystem für das entsprechende Netzwerk des Kundenunternehmens bereitzustellen, zu verwalten und zu warten.

- *Mandant*. Kundenunternehmen, dessen Geräte geschützt werden sollen.

- *Verwaltete Geräte*. Von Kaspersky Next Expert View Linux geschützte Geräte des Kundenunternehmens. Auf jedem der zu schützenden Geräte muss der Administrationsagent und eine der Kaspersky-Sicherheitsanwendungen installiert sein.

- *Verwaltetes Gerät, das als Verteilungspunkt fungiert*. Computer, auf dem der Administrationsagent installiert ist und der zur Update-Verteilung, Netzwerkabfrage, Remote-Installation von Programmen und zum Empfangen von Informationen über Computer in einer Administrationsgruppe und/oder Broadcasting-Domäne verwendet wird. Der Administrator wählt die entsprechenden Geräte aus und weist sie manuell als Verteilungspunkte zu. Verteilungspunkte können auch als Verbindungs-Gateways fungieren, um die Anzahl der ausgehenden externen Verbindungen und der gleichzeitigen Verbindungen zum Administrationsserver zu reduzieren. Es wird empfohlen, die Anzahl der verwalteten Computer zu begrenzen, die sich direkt mit dem Administrationsserver verbinden.

Szenario: Bereitstellung des Schutzes (Verwaltung von Mandanten mittels virtueller Administrationsserver)

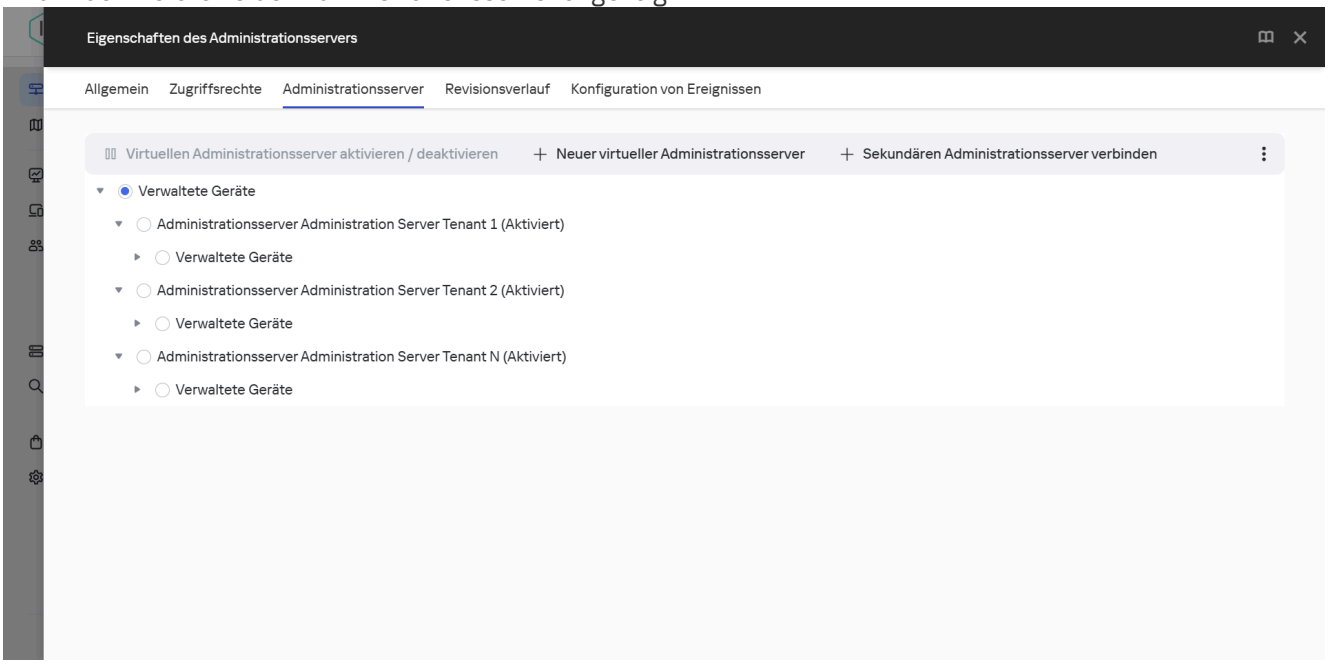
Wenn Sie Kaspersky Security Center noch nie verwendet haben und Sie Ihre Mandanten über virtuelle Administrationsserver verwalten möchten, gehen Sie wie in diesem Abschnitt beschrieben vor. Wenn Sie das Szenario abgeschlossen haben, werden die Geräte Ihrer Kunden geschützt.

Wenn Sie mehrere Mandanten verwalten, führen Sie dieses Szenario für jeden Mandanten separat durch.

Das Szenario verläuft in den folgenden Schritten:

1. **Einen virtuellen Administrationsserver erstellen**

   Erstellen Sie einen virtuellen Administrationsserver für Ihren Kunden. Der neue virtuelle Administrationsserver wird in der Hierarchie der Administrationsserver angezeigt:



Virtueller Administrationsserver in der Hierarchie der Administrationsserver

2. **Ein Gerät als Verteilungspunkt auswählen**

   Legen Sie basierend auf allen Geräten eines des Kunden fest, welches Gerät als Verteilungspunkt fungieren soll.

   > Sie können nicht mehr als 100 Verteilungspunkte in einem Arbeitsbereich betreiben.

3. **Ein autonomes Installationspaket für den Administrationsagenten erstellen**

   Wechseln Sie zum erstellten virtuellen Administrationsserver und erstellen Sie anschließend ein autonomes Installationspaket für den Administrationsagenten. Sie können die Administrationsserver im Hauptmenü wechseln, indem Sie auf das Chevron-Symbol (›) rechts neben dem Namen des aktuellen Administrationsservers klicken und anschließend den benötigten Administrationsserver auswählen. Geben Sie während der Erstellung des autonomen Installationspakets eine Administrationsgruppe für verwaltete Geräte an, in die das Gerät verschoben werden soll.

4. **Installieren des Administrationsagenten auf dem ausgewählten Gerät, das als Verteilungspunkt fungieren soll**

   Sie können die für Sie am besten geeignete Methode verwenden:

   - Manuelle Installation

     Um ein autonomes Installationspaket an ein Gerät auszuliefern, können Sie es beispielsweise auf einen Wechseldatenträger (z. B. ein Flash-Laufwerk) kopieren oder es in einem freigegebenen Ordner platzieren.

   - Bereitstellung unter Verwendung von Active Directory

   - Bereitstellung unter Verwendung einer RMM-Softwarelösung Ihrer Wahl (Remote Monitoring and Management)

5. **Einen Verteilungspunkt zuweisen**

   Weisen Sie dem Gerät mit installiertem Administrationsagent die Rolle des Verteilungspunkts zu.

6. **Netzwerkabfrage**

   Konfigurieren und Durchführen von Netzwerkabfragen mittels Verteilungspunkt.

   Kaspersky Next Expert View stellt die folgenden Methoden für Netzwerkabfragen zur Verfügung:

   - IP-Bereiche abfragen

   - Windows-Netzwerkabfrage

   - Abfrage der Active Directory

   Wenn die Netzwerkabfrage nach Zeitplan abgeschlossen ist, sind die Geräte Ihres Kunden entdeckt und wurden in die Gruppe **Nicht zugeordnete Geräte** verschoben.

7. **Verschieben von entdeckten Geräten in Administrationsgruppen**

   Legen Sie Regeln für das automatische Verschieben von entdeckten Geräten in die vorgesehenen Administrationsgruppen fest oder verschieben Sie diese Geräte manuell in die vorgesehenen Administrationsgruppen. Wenn Sie die Geräte des Kunden in einer einzigen Administrationsgruppe verwalten möchten, können Sie die Geräte in die Gruppe "Verwaltete Geräte" verschieben.

8. **Installationspakete für den Administrationsagenten und für verwaltete Kaspersky-Anwendungen erstellen**

   Erstellen Sie Installationspakete für Kaspersky-Anwendungen.

9. **Entfernen der Sicherheitsanwendung von Drittanbietern.**

   Wenn Sicherheitsanwendungen von Drittanbietern auf den Geräten Ihrer Kunden installiert sind, entfernen Sie diese vor der Installation von Kaspersky-Anwendungen.

10. **Kaspersky-Anwendungen auf Client-Geräten installieren**

    Erstellen Sie Aufgaben zur Remote-Installation, um den Administrationsagenten und verwaltete Kaspersky-Anwendungen auf Ihren Kundengeräten zu installieren.

    Wenn benötigt, können Sie auch mehrere Aufgaben zur Remote-Installation zum Installieren von verwalteten Kaspersky-Anwendungen für verschiedene Administrationsgruppen oder für unterschiedliche Geräteauswahlen erstellen.

    Nachdem die Aufgaben erstellt wurden, können Sie die Einstellungen konfigurieren. Stellen Sie sicher, dass der Zeitplan für jede erstellte Aufgabe Ihren Anforderungen entspricht. Zunächst muss die Aufgabe zum Installieren des Administrationsagenten ausgeführt werden. Nachdem der Administrationsagent auf den Geräten Ihres Kunden installiert wurde, muss die Aufgabe zum Installieren von verwalteten Kaspersky-Anwendungen ausgeführt werden.

11. **Überprüfung der Erstbereitstellung von Kaspersky-Anwendungen**

    Lassen Sie sich den **Bericht über Versionen der Kaspersky-Anwendungen** generieren und anzeigen. Stellen Sie sicher, dass die verwalteten Kaspersky-Anwendungen auf allen Geräten Ihres Kunden installiert sind.

12. **Erstellen von Richtlinien für Kaspersky-Anwendungen**

    Erstellen Sie eine Richtlinie für die benötigte Kaspersky-Anwendung. Wenn Sie eine universelle Richtlinie für alle Ihre Kunden erstellen möchten, wechseln Sie von dem aktuellen virtuellen Administrationsserver auf den primären Administrationsserver und erstellen Sie dann eine Richtlinie für die gewünschte Kaspersky-Anwendung.

Szenario: Bereitstellung des Schutzes (Verwaltung von Mandanten mittels Administrationsgruppen)

Wenn Sie Kaspersky Security Center noch nie verwendet haben und Ihre Mandanten über Administrationsgruppen verwalten möchten, gehen Sie wie in diesem Abschnitt beschrieben vor. Wenn Sie das Szenario abgeschlossen haben, werden die Geräte Ihrer Kunden geschützt.

Das Szenario verläuft in den folgenden Schritten:

1. **Administrationsgruppen anlegen**

   Erstellen einer Administrationsgruppe für jeden Ihrer Kunden.

2. **Struktur der Verteilungspunkte planen**

   Basierend auf allen Geräten eines jeden Kunden festlegen, welche Geräte als Verteilungspunkte fungieren sollen.

   > Sie können nicht mehr als 100 Verteilungspunkte in einem Arbeitsbereich betreiben.

3. **Ein autonomes Installationspaket für den Administrationsagenten erstellen**

   Erstellen eines autonomen Installationspakets für den Administrationsagenten.

4. **Installieren des Administrationsagenten auf den ausgewählten Geräten, die als Verteilungspunkte fungieren sollen**

Installieren Sie den Administrationsagenten auf den ausgewählten Geräten, die als Verteilungspunkte fungieren sollen.

Sie können die für Sie am besten geeignete Methode verwenden:

- Manuelle Installation

  Um ein autonomes Installationspaket an Geräte auszuliefern, können Sie es beispielsweise auf einen Wechseldatenträger (z. B. ein Flash-Laufwerk) kopieren oder es in einem freigegebenen Ordner platzieren

- Bereitstellung unter Verwendung von Active Directory

- Bereitstellung unter Verwendung einer RMM-Softwarelösung Ihrer Wahl (Remote Monitoring and Management)

5. **Verteilungspunkte zuweisen**

   Zuweisen eines Verteilungspunktes an Geräte, auf denen der Administrationsagent installiert ist.

6. **Netzwerkabfrage**

   Konfigurieren und Durchführen von Netzwerkabfragen mittels Verteilungspunkt.

   Kaspersky Next Expert View stellt die folgenden Methoden für Netzwerkabfragen zur Verfügung:

   - IP-Bereiche abfragen
   - Windows-Netzwerkabfrage
   - Abfrage der Active Directory

   Wenn die Netzwerkabfrage nach Zeitplan abgeschlossen ist, sind die Geräte Ihres Kunden entdeckt und wurden in die Gruppe **Nicht zugeordnete Geräte** verschoben.

7. **Verschieben von entdeckten Geräten in Administrationsgruppen**

   Legen Sie Regeln für das automatische Verschieben von entdeckten Geräten in die vorgesehenen Administrationsgruppen fest, oder verschieben Sie diese Geräte manuell in die vorgesehenen Administrationsgruppen.

8. **Installationspakete für den Administrationsagenten und für verwaltete Kaspersky-Programme erstellen**

   Wenn Sie den Schnellstartassistenten nicht ausgeführt oder den Schritt zum Erstellen von Installationspaketen übersprungen haben, erstellen Sie Installationspakete für Kaspersky-Anwendungen.

9. **Entfernen der Sicherheitsanwendung von Drittanbietern.**

   Wenn Sicherheitsanwendungen von Drittanbietern auf den Geräten Ihrer Kunden installiert sind, entfernen Sie diese vor der Installation von Kaspersky-Anwendungen.

10. **Installieren von Kaspersky-Anwendungen auf den Geräten Ihrer Kunden**

    Erstellen Sie Aufgaben zur Remote-Installation, um den Administrationsagenten und verwaltete Kaspersky-Anwendungen auf Ihren Kundengeräten zu installieren.

    Wenn benötigt, können Sie auch mehrere Aufgaben zur Remote-Installation zum Installieren von verwalteten Kaspersky-Anwendungen für verschiedene Administrationsgruppen oder für unterschiedliche Geräteauswahlen erstellen.

    Nachdem die Aufgaben erstellt wurden, können Sie die Einstellungen konfigurieren. Stellen Sie sicher, dass der Zeitplan für jede erstellte Aufgabe Ihren Anforderungen entspricht. Zunächst muss die Aufgabe zum Installieren des Administrationsagenten ausgeführt werden. Nachdem der Administrationsagent auf den Geräten Ihres Kunden installiert wurde, muss die Aufgabe zum Installieren von verwalteten Kaspersky-Anwendungen ausgeführt werden.

11. **Überprüfung der Erstbereitstellung von Kaspersky-Anwendungen**

    Lassen Sie sich den **Bericht über Versionen der Kaspersky-Anwendungen** generieren und anzeigen. Stellen Sie sicher, dass die verwalteten Kaspersky-Anwendungen auf allen Geräten Ihrer Kunden installiert sind.

12. **Erstellen von Richtlinien für Kaspersky-Anwendungen**

    Rufen Sie das Menü **Asset-Verwaltung** → **Gruppen** auf. Wenn Sie eine universelle Richtlinie für alle Ihre Kunden erstellen möchten, wählen Sie **Administrationsserver aus.** Wenn Sie eine spezifische Richtlinie für einen individuellen Kunden erstellen möchten, wählen Sie die Ihrem Kunden entsprechende Administrationsgruppe aus. Erstellen Sie eine Richtlinie für die benötigte Kaspersky-Anwendung.

Gemeinsame Verwendung von einem lokal ausgeführten Kaspersky Security Center und Kaspersky Next Expert View

Wenn Sie bereits ein lokal ausgeführtes Kaspersky Security Center verwenden, können Sie Ihre existierenden und lokal ausgeführten Administrationsserver in sekundäre Administrationsserver Ihres neuen Administrationsservers von Kaspersky Next Expert View konvertieren, wie in diesem Abschnitt beschrieben.

Wenn Sie die gemeinsame Verwendung von einem lokal ausgeführten Kaspersky Security Center und Kaspersky Next Expert View konfigurieren, können Sie nur dann von einem lokalen Kaspersky Security Center auf Kaspersky Next Expert View migrieren, wenn Sie die Hierarchie der Administrationsserver entfernen.

Um eine Hierarchie von Administrationsservern zu erstellen:

fügen Sie Ihre existierenden und lokal ausgeführten Administrationsserver als sekundäre Administrationsserver hinzu.

Lizenzierung von Kaspersky-Programmen für Managed Service Provider (MSPs)

Kaspersky Next Expert View ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Anwendungen auf den Geräten Ihrer Kunden sowie die Überwachung der Schlüsselverwendung und die Verlängerung der Gültigkeitsdauer der Lizenz.

Wenn Sie mehrere Mandanten verwalten, können Sie die Lizenzschlüssel auf folgende Arten verteilen:

- Einen Lizenzschlüssel für alle Mandanten.
- Einen individuellen Lizenzschlüssel für jeden Mandanten.

Um Lizenzschlüssel auf den Geräten Ihrer Kunden zu verteilen:

1. Fügen Sie die benötigten Lizenzschlüssel der Datenverwaltung des Administrationsservers hinzu.
2. Führen Sie eine der folgenden Aktionen aus:

   - Konfigurieren Sie die automatische Verteilung eines Lizenzschlüssels.

     In diesem Fall wählt Kaspersky Next Expert View einen der anwendbaren Lizenzschlüssel aus und verteilt diesen jedes Mal automatisch, sobald ein neues Gerät entdeckt wird.

   - Konfigurieren Sie eine Aufgabe zum Hinzufügen eines Schlüssels, um einen Lizenzschlüssel an Geräte zu verteilen.

     Während der Konfiguration der Aufgabe wählen Sie den Lizenzschlüssel, der an Geräte verteilt werden soll, und die Administrationsgruppe mit den entsprechenden Geräten, aus.

     Eine Aufgabe kann jeweils nur einen Lizenzschlüssel verteilen. Dies bedeutet für den Fall, dass Sie mehrere Lizenzschlüssel verteilen wollen, die Erstellung einer Aufgabe für jeden Schlüssel.

Die auf den Geräten Ihres Kunden installierten Kaspersky-Anwendungen sind aktiviert.

Das Hinzufügen eines aktiven Lizenzschlüssels zum primären Administrationsserver ist obligatorisch. Andernfalls wird der zugehörige Arbeitsbereich nach 90 Tagen gelöscht. Dies geschieht unabhängig vom Status der Lizenzschlüssel auf anderen Administrationsservern innerhalb dieses Arbeitsbereichs.

Überwachungs- und Berichtsfunktionen für Managed Service Provider (MSPs)

Kaspersky Next Expert View stellt Ihnen Möglichkeiten für die Überwachung und Berichterstattung zur Verfügung. Diese Möglichkeiten geben Ihnen einen Überblick über die Infrastruktur, die Zustände des Schutzstatus und die Statistiken von Ihrer Organisation.

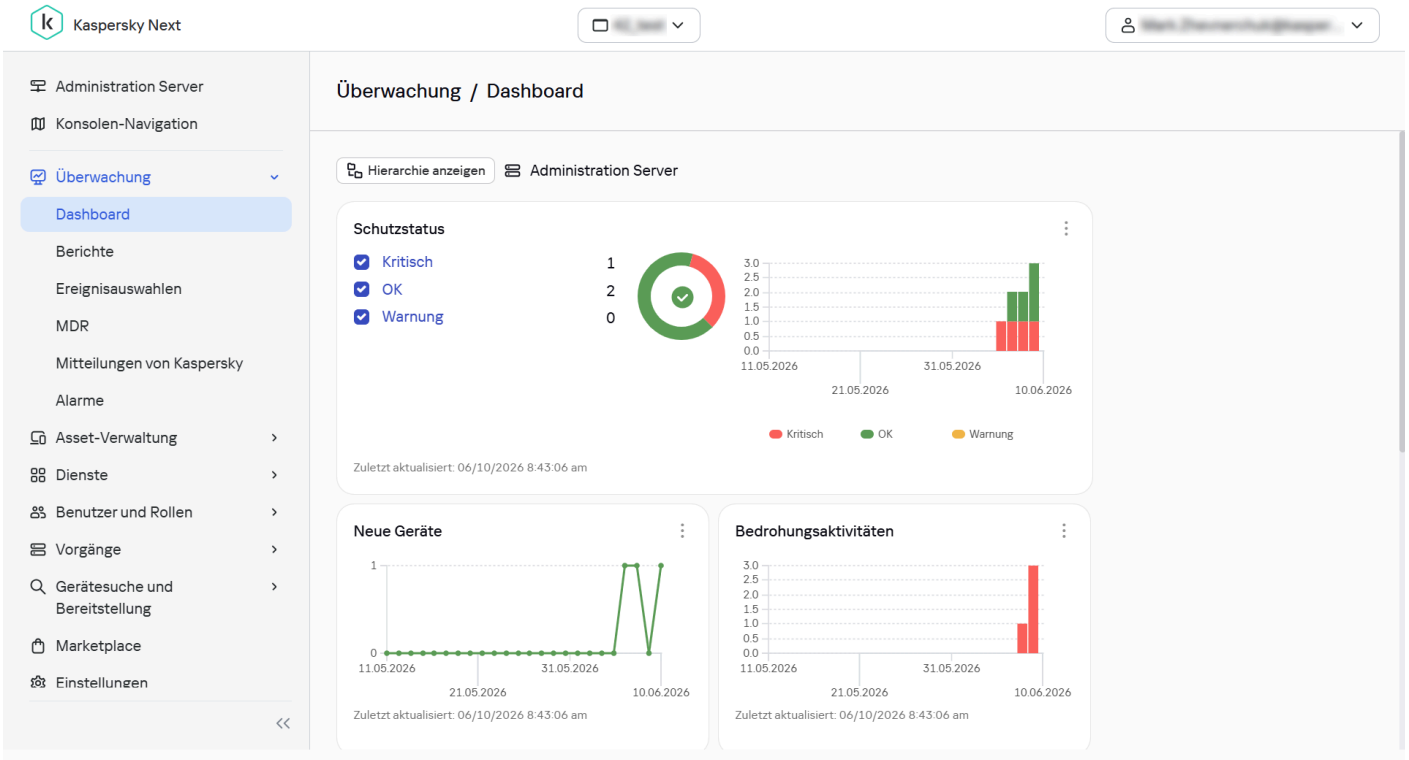
Wenn Sie Kaspersky Next Expert View bereitgestellt haben, können Sie die Funktionen zur Überwachung und Berichterstattung konfigurieren, um sie an Ihre Bedürfnisse anzupassen.

Kaspersky Next Expert View stellt die folgenden Funktionen zur Überwachung und Berichterstattung zur Verfügung:

- Dashboard
- Berichte
- Ereignisauswahlen
- E-Mail-Benachrichtigungen

Dashboard

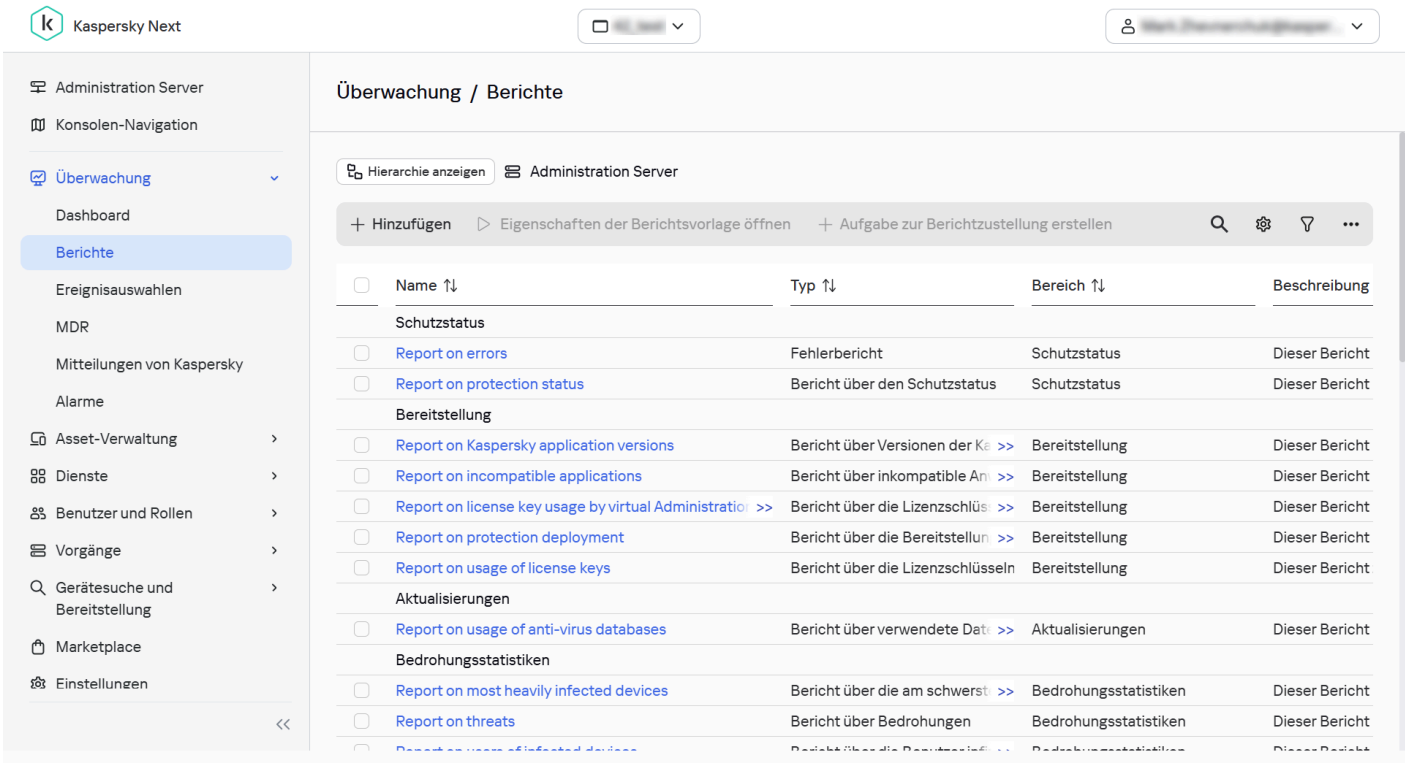
Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen (Siehe Abbildung unten).



Der Dashboard-Abschnitt

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. Sie können außerdem einen Zeitplan festlegen, nach dem Berichte versandt werden sollen (siehe Abbildung unten).



Der Berichts-Abschnitt

Ereignisauswahlen

Die Ereignisauswahlen bieten eine Bildschirmansicht der benannten Ereignisgruppen, die aus der Administrationsserver-Datenbank ausgewählt wurden. Kaspersky Next Expert View enthält bereits einige vordefinierte Ereignisauswahlen (zum Beispiel **Letzte Ereignisse** und **Kritische Ereignisse**). Sie können außerdem benutzerdefinierte Ereignisauswahlen erstellen.

E-Mail-Benachrichtigungen

Sie können E-Mail-Benachrichtigungen konfigurieren, um über Ereignisse, die in Kaspersky Next Expert View und auf Ihren Kundengeräten auftreten, informiert zu werden.

Arbeiten mit Kaspersky Next Expert View in einer Cloud-Umgebung

Dieser Abschnitt bietet Informationen zu Kaspersky Next Expert View in Bezug auf den Betrieb und die Wartung von Kaspersky Next Expert View 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, sind die Bedienelemente mit Bezug zu Cloud-Geräten nicht bedienbar.

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.

Varianten der Lizenzierung in der Cloud-Umgebung

Das Arbeiten in einer Cloud-Umgebung ist sowohl im Testmodus als auch kommerziellen Modus der Kaspersky Next Expert View möglich:

- Im Testmodus sind während des gesamten Gültigkeitszeitraums alle Funktionen der Cloud-Umgebung in Ihrem Arbeitsbereich verfügbar. Es ist keine Lizenz erforderlich.
- Im kommerziellen Modus sind die Funktionen der Cloud-Umgebung nur dann verfügbar, wenn in den Eigenschaften des Administrationsservers ein aktiver Lizenzschlüssel für Kaspersky Hybrid Cloud Security hinzugefügt wurde.

In beiden Fällen wird das Schwachstellen- und Patch-Management automatisch aktiviert.

Wenn beim Aktivieren der Funktion "Arbeit in der Cloud-Umgebung" mittels Lizenz für Kaspersky Hybrid Cloud Security ein Fehler auftritt, verwenden Sie die Schlüsseldatei.

Vorbereitung auf das Arbeiten in einer Cloud-Umgebung mittels Kaspersky Next Expert View

In diesem Abschnitt erfahren Sie, wie Sie sich für die Arbeit mit Kaspersky Next Expert View in den folgenden Cloud-Umgebungen vorbereiten:

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Arbeit mit der Cloud-Umgebung Amazon Web Services

In diesem Abschnitt erfahren Sie, wie Sie sich für die Arbeit mit Kaspersky Next Expert View in Amazon Web Services vorbereiten.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Next Expert View aktuell.

Über die Arbeit in der Cloud-Umgebung Amazon Web Services

Für die Arbeit mit der AWS-Plattform und insbesondere, um 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.

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 Next Expert View aktuell.

Erstellen von IAM-Benutzerkonten für Amazon EC2-Instances

In diesem Abschnitt werden die Aktionen beschrieben, die durchgeführt werden müssen, um einen ordnungsgemäßen Betrieb der Kaspersky Next Expert View zu gewährleisten. Diese Aktionen umfassen Arbeiten mit den AWS-Idendity-Benutzerkonten, sowie mit den Benutzerkonten der Zugriffsverwaltung (IAM). Ferner werden die Aktionen beschrieben, die auf Client-Geräten unternommen werden müssen, um darauf den Administrationsagenten zu installieren und anschließend Kaspersky Endpoint Security für Linux zu installieren.

Sicherstellen der Berechtigungen zur Arbeit der Kaspersky Next Expert View mit AWS

Um in der Cloud-Umgebung von Amazon Web Services mit Kaspersky Next Expert View zu arbeiten, müssen Sie ein *IAM-Benutzerkonto* erstellen, welches von Kaspersky Next Expert View für die Arbeit mit AWS-Diensten verwendet wird. 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 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.

Erstellen eines IAM-Benutzerkontos für die Arbeit mit Kaspersky Next Expert View

Für die Arbeit mit der Kaspersky Next Expert View ist ein IAM-Benutzerkonto erforderlich. 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 Next Expert View 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:

- https://docs.aws.amazon.com/de_de/IAM/latest/UserGuide/introduction.html.
- https://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** aus.

   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.
   - Berechtigung: **ReadOnlyAccess**.

     Nachdem Sie Berechtigung 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.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Next Expert View aktuell.

Arbeiten mit der Cloud-Umgebung Microsoft Azure

Dieser Abschnitt informiert über den Betrieb und die Wartung von Kaspersky Next Expert View in einer Cloud-Umgebung, die von Microsoft Azure bereitgestellt wird, sowie über die Bereitstellung des Schutzes auf virtuellen Maschinen in dieser Cloud-Umgebung.

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. Erstellen Sie eine Azure Anwendungs-ID mit den für die Installation von Anwendungen auf virtuellen Maschinen erforderlichen Berechtigungen, bevor Sie mit Microsoft Azure in Kaspersky Next Expert View arbeiten.

Erstellen eines Abonnements, einer Anwendungs-ID und eines Kennworts

Zum Arbeiten mit Kaspersky Next Expert View in der Microsoft Azure-Umgebung benötigen Sie ein Azure-Abonnement, eine Azure Anwendungs-ID 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 Next Expert View 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 Next Expert View 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 Next Expert View 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 mithilfe der Azure-API nicht nur finden, sondern auch schützen möchten, muss Ihre Azure Anwendungs-ID über die Rolle "Virtual Machine Contributer" verfügen.

Befolgen Sie die Anleitung auf der Microsoft-Website, um Ihrer Azure Anwendungs-ID eine Rolle zuzuweisen.

Arbeiten mit Google Cloud

Dieser Abschnitt enthält Informationen über das Arbeiten mit Kaspersky Next Expert View in einer von Google bereitgestellten Cloud-Umgebung.

Sie können die Google API verwenden, um mit Kaspersky Next Expert View 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 Kaspersky Next Expert View 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.

Der Assistent für das Konfigurieren der Cloud-Umgebung in Kaspersky Next Expert View

Um Kaspersky Next Expert View mithilfe dieses Assistenten zu konfigurieren, müssen Sie über Folgendes verfügen:

- Spezifische Anmeldeinformationen für eine Cloud-Umgebung:
  - Ein IAM-Benutzerkonto, dem das Recht eingeräumt wurde, das Cloud-Segment abzufragen (für die Arbeit 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- oder Linux-Server

Wenn Ihr Arbeitsbereich unter Verwendung einer Lizenz für Kaspersky Hybrid Cloud Security erstellt wurde, wird der Assistent für das Konfigurieren der Cloud-Umgebung automatisch bei der ersten Verbindung mit Kaspersky Next Expert View gestartet. Wenn Sie den Assistenten für das Konfigurieren der Cloud-Umgebung überspringen, wird dieser bei jeder Verbindung mit Kaspersky Next Expert View gestartet, bis Sie alle Schritte des Assistenten abgeschlossen haben.

Sie können den Assistenten für das Konfigurieren der Cloud-Umgebung auch jederzeit manuell starten.

Um den Assistenten für das Konfigurieren der Cloud-Umgebung manuell zu starten, gehen Sie wie folgt vor,

Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Konfigurieren der Cloud-Umgebung**.

Der Assistent wird gestartet.

Eine durchschnittliche Arbeitssitzung mit diesem Assistenten dauert etwa 15 Minuten.

Wenn Sie den Administrationsserver nicht unter der Lizenz für Kaspersky Hybrid Cloud Security aktiviert haben, müssen Sie dies im ersten Schritt des Assistenten tun.

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
- Installationspaket und Web-Plug-in für Kaspersky Endpoint Security für Windows

Kaspersky Next Expert View 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. Auswählen der Methode zur Programmaktivierung

Dieser Schritt wird nur angezeigt, wenn Sie während der Erstellung des Arbeitsbereichs keine Lizenz von Kaspersky Hybrid Cloud Security angegebenen haben, und wenn Sie keinen Lizenzschlüssel für Kaspersky Hybrid Cloud Security im Aktivierungsfeld des Administrationsservers hinzugefügt haben. In diesem Fall müssen Sie den Administrationsserver unter Verwendung einer Lizenz für Kaspersky Hybrid Cloud Security aktivieren.

Schritt 3. Auswählen der Cloud-Umgebung und Autorisierung

Geben Sie die folgenden Einstellungen an:

- **Cloud-Umgebung**

  Wählen Sie die Cloud-Umgebung aus, in der Sie Kaspersky Next Expert View bereitstellen: AWS, Azure oder Google Cloud.

  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, verwenden Sie einen AWS IAM-Zugriffsschlüssel, um das Cloud-Segment weiter abzufragen. Geben Sie die folgenden Daten des Schlüssels 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, nachdem Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel 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, nachdem Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel 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:

- **Azure Anwendungs-ID**

  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.

- **Kennwort der Azure-Anwendung**

  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 Next Expert View zu arbeiten.

- **Zugriffsschlüssel für Azure-Speicher**

  Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Next Expert View erstellt haben.

  Sie finden den Schlüssel im Azure-Speicherkonto im Abschnitt "Übersicht" 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.

Der Assistent für das Konfigurieren der Cloud-Umgebung erlaubt Ihnen nur die Angabe eines Segments. Sie können später weitere Verbindungen für die Verwaltung anderer Cloud-Segmente angeben.

Klicken Sie auf **Weiter** um fortfahren.

Schritt 4. Abfragen des Segments und Konfiguration der Synchronisierung mit der Cloud

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 fünf 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.

Definieren der Einstellung **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 es, 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 Next Expert View 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.

Klicken Sie auf **Weiter** um fortfahren.

Schritt 5. Konfiguration von Kaspersky Security Network für Kaspersky Next Expert View

Dieser Schritt wird übersprungen, wenn Sie Kaspersky Next Expert View im Testmodus oder auf einem virtuellen Administrationsserver ausführen.

Legen Sie die Einstellungen für das Übertragen von Informationen über die Ausführung von Kaspersky Next Expert View in die Wissensdatenbank von Kaspersky Security Network (KSN) fest. Wählen Sie eine der folgenden Varianten aus:

- **Ich stimme der Teilnahme an Kaspersky Security Network zu**

  Kaspersky Next Expert View und die verwalteten Programme, die auf Client-Geräten installiert sind, übertragen ihre Betriebsdetails 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 Teilnahme an Kaspersky Security Network ab**

  Kaspersky Next Expert View 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 6. 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 Next Expert View

Daten über die Netzwerkstruktur (und der darin befindlichen Geräte) werden anhand von regelmäßigen Abfragen der Cloud-Segmente durch die Tools der AWS-API, Azure-API oder Google-API erhalten. Auf Grundlage der empfangenen Daten aktualisiert Kaspersky Next Expert View 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 sind entsprechende Rechte erforderlich, die mit einem IAM-Benutzerkonto (in AWS), mit 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 über Kaspersky Next Expert View

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 Cloud Console bereitstellen: AWS, Azure oder Google Cloud.

     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 Folgendes an:

     - **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, nachdem Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel 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, nachdem Sie für die Autorisierung den AWS IAM-Zugriffsschlüssel 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:

  - **Azure Anwendungs-ID**

    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.

  - **Kennwort der Azure-Anwendung**

    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 Next Expert View zu arbeiten.

  - **Zugriffsschlüssel für Azure-Speicher**

    Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Next Expert View erstellt haben.

    Sie finden den Schlüssel im Azure-Speicherkonto im Abschnitt "Übersicht" 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 mittels Kaspersky Next Expert View anpassen

Die Abfrage des Cloud-Segments erfolgt nach Zeitplan. Sie können das Intervall festlegen, in dem die Abfrage durchgeführt wird.

Während der Ausführung des Assistenten für das Konfigurieren der Cloud-Umgebung wird als Intervall für die Abfrage automatisch einmal in fünf 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 fünf 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.

   - **Startintervall (Tage)**

     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 Ihr Arbeitsbereich während der für die Abfrage geplanten Zeit nicht verfügbar ist, kann Kaspersky Next Expert View die Abfrage entweder sofort starten, nachdem er wieder verfügbar ist, oder auf die nächste planmäßige Durchführung warten.

     Wenn diese Option aktiviert ist, beginnt Kaspersky Next Expert View sofort mit der Abfrage, nachdem der Arbeitsbereich wieder verfügbar ist.

Wenn diese Option deaktiviert ist, wartet Kaspersky Next Expert View auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

Diese Option ist standardmäßig aktiviert.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Der Abfragezeitplan für das Segment wurde konfiguriert und gespeichert.

Anzeigen der Ergebnisse der Abfrage des Cloud-Segments durch Kaspersky Next Expert View

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**.

Die für die Abfrage verfügbaren Cloud-Segmente werden angezeigt.

Anzeigen der Eigenschaften von Cloud-Geräten mittels Kaspersky Next Expert View

Sie können die Eigenschaften jedes Cloud-Geräts anzeigen.

Um die Eigenschaften eines Cloud-Gerätes anzuzeigen:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Assets (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

Während der Ausführung des Assistenten für das Konfigurieren der Cloud-Umgebung wird automatisch die Regel zur Synchronisierung mit Cloud 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**.

   Die Liste mit Verschiebungsregeln öffnet sich.

2. Wählen Sie in der Liste mit Verschiebungsregeln **Mit der Cloud synchronisieren** aus.

   Das Eigenschaftenfenster der Regel wird 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 Next Expert View 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 Next Expert View 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 Verwendung des Assistenten für das Konfigurieren 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 mit Kaspersky Next Expert View 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 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 aus irgendwelchen Gründen für die Suche mithilfe API nicht auffindbar.

   - **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.
- 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 Next Expert View 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
- 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 Next Expert View unterstützt werden.

So erstellen Sie eine Aufgabe zur Remote-Installation eines Programms auf virtuellen Maschinen von Azure:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Folgen Sie den Schritten des Assistenten:
   a. Wählen Sie den Aufgabentyp **Remote-Installation einer Anwendung** 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.

- **Azure Anwendungs-ID**

  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.

- **Kennwort der Azure-Anwendung**

  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.

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 Next Expert View noch in den anderen Informationsquellen zu Kaspersky Next Expert View 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 Next Expert View.

Kaspersky bietet den Support für Kaspersky Next Expert View in Übereinstimmung mit dem Lebenszyklus der Anwendung an (siehe Seite mit den Lebenszyklen unserer Anwendungen). 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.

Hilfreiche Informationen für die Spezialisten des Technischen Supports von Kaspersky

Wenn Sie die Spezialisten des Technischen Supports von Kaspersky kontaktieren, können diese die folgenden Informationen von Ihnen abfragen:

- Allgemeine Informationen über Kaspersky Next Expert View
- ID des Arbeitsbereichs
- Lizenzinformation
- Anzahl der installierten Programme
- Mandanten-ID und -Status

Sie finden diese Informationen in Web Console, indem Sie auf Ihren Kontonamen klicken und in der Dropdown-Liste die Schaltfläche **Support** auswählen. Die Registerkarte **Allgemein** enthält Informationen über Ihren Arbeitsbereich, die Lizenzierung und installierte Anwendungen. Kopieren Sie diese Informationen und geben Sie sie an die Spezialisten des Technischen Supports von Kaspersky weiter, um Hilfe zu Ihrem Problem zu erhalten.

Informationsquellen über das Programm

Seite von Kaspersky Next Expert View auf der Website von Kaspersky

In dem Abschnitt zu Kaspersky Next Expert View auf der Kaspersky-Website finden Sie allgemeine Informationen über die Anwendung, ihre Funktionen und Besonderheiten.

Seite von Kaspersky Next Expert View in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt der Website des Technischen Supports von Kaspersky.

In dem Abschnitt von Kaspersky Next Expert View 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 Next Expert View 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.

Bekannte Probleme

Kaspersky Next Expert View hat eine Reihe von Einschränkungen, die für die Verwendung des Programms nicht kritisch sind:

- Der Wechsel von Expert View zu Pro View ist derzeit nicht möglich.
- Wenn Sie einen Benutzer vom primären Administrationsserver zu einem virtuellen Administrationsserver hinzufügen, wird dem Benutzer automatisch die Rolle „Hauptadministrator“ zugewiesen.

  Wenn Sie einem Benutzer benutzerdefinierte Rechte zuweisen möchten (z. B. nur das Recht **Lesen** gewähren möchten), navigieren Sie zu den **Eigenschaften des Administrationsservers**. Wählen Sie auf der Registerkarte **Zugriffsrechte** Benutzer und einen virtuellen Administrationsserver aus und überspringen Sie anschließend den Schritt zur Rollenzuweisung. Die Benutzer werden dem virtuellen Administrationsserver hinzugefügt, verfügen jedoch über keinerlei Rechte auf diesem Server. Um einem Benutzer benutzerdefinierte Rechte zuzuweisen, navigieren Sie zu den Eigenschaften des virtuellen Administrationsservers, wählen Sie die Benutzer aus und weisen Sie ihnen anschließend benutzerdefinierte Rechte zu.
- Wenn Sie unter **Asset-Verwaltung** → **Aufgaben** den Filter in der Spalte **Aufgabentyp** auswählen, wird in der Dropdown-Liste möglicherweise ein falscher Wert angezeigt.
- Die Richtlinienliste wird beim Ändern der Größe des Browserfensters nicht korrekt angezeigt.
- In den Abschnitten **Richtlinien** und **Aufgaben** ist die Gruppierung nach Anwendungen standardmäßig nicht aktiviert.
- Wenn Sie wiederholt von Pro View zu Expert View wechseln, werden Richtlinien für verwaltete Anwendungen mit doppelten Namen erstellt.
- Wenn der Administrationsagent unter Windows XP installiert ist, sind keine Informationen über verwaltete Anwendungskomponenten verfügbar.
- Ein Installationspaket kann nur einmal in einer bestimmten Lokalisierungssprache hinzugefügt werden. Wenn Sie beispielsweise das Installationspaket für Kaspersky Endpoint Security für Windows (Deutsch) bereits hinzugefügt haben, können Sie weitere Installationspakete von Kaspersky Endpoint Security für Windows in anderen Sprachen hinzufügen. Das Paket für Deutsch können Sie jedoch nicht noch einmal hinzufügen.
- Wenn Sie im Fenster **Alarm-Details** einen beliebigen Link anklicken, der einen anderen Abschnitt öffnet, und dann versuchen zurückzukehren und die **Zurück**-Schaltfläche Ihres Browsers klicken (oder **`Alt`**+**`Pfeil nach links`** drücken), verfällt das Fenster **Alarm-Details** in eine Ladeschleife.
- Wenn als Sprache vereinfachtes Chinesisch ausgewählt ist, werden die Informationen in den Abschnitten **Überwachung** → **MDR**, **Einstellungen** → **Integration** → **Kaspersky EDR Expert** und **Asset-Verwaltung** → **Mobile Geräte** möglicherweise fehlerhaft dargestellt.
- 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 versuchen, sich mit Active Directory Federation Services (AD FS) an der Kaspersky Next Expert View anzumelden, aber die erforderlichen Berechtigungen fehlen, gibt die Kaspersky Next Expert View immer noch den Fehler "Ungültige Anmeldedaten" zurück, anstatt den Benutzer über fehlende Berechtigungen zu warnen.

- Für macOS-Geräten wird die Aufgabe zur Verwaltung der Geräte nicht ordnungsgemäß ausgeführt.
- Im Fenster für die Ferndiagnose kann das Klicken der Schaltfläche **Vollständige Datei herunterladen** zu einem fehlerhaften Download führen.
- Ignorierte Schwachstellen von Drittanbietern (Software von Microsoft nicht eingeschlossen) wird im Diagramm **Statistik zu Schwachstellen auf Geräten** nicht angezeigt.

Glossar

Administrationsagent

Eine Komponente von Kaspersky Next Expert View, mit deren Hilfe die Interaktion zwischen dem Administrationsserver und den Kaspersky-Anwendungen ermöglicht wird, die auf einem bestimmten Netzwerk-Node (Workstation oder Server) installiert sind. Diese Komponente ist für alle von dem Unternehmen entwickelten Programme 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 Next Expert View, die Informationen über alle Kaspersky-Anwendungen, die innerhalb des Unternehmensnetzwerks installiert sind, zentral speichert. Sie kann auch zur Verwaltung dieser Programme verwendet werden.

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.

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.

Arbeitsbereich

Eine Instanz von Kaspersky Next, die für ein bestimmtes Unternehmen erstellt wurde. Wenn von einem Kunden ein Arbeitsbereich angelegt wird, erstellt und konfiguriert Kaspersky die Infrastruktur und cloudbasierte Verwaltungskonsole, die für die Verwaltung von auf Geräten des Unternehmens installierten Sicherheitsanwendungen benötigt werden.

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)

Die Schnittstelle zur Anwendungsprogrammierung für die AWS-Plattform, die von Kaspersky Next Expert View verwendet wird. Die Tools der AWS-API werden insbesondere für die Abfrage von Cloud-Segmenten 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.

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.

Cloud Discovery

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 *Dateifreigabe*, *Messenger* oder *E-Mail* eingeteilt.

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 Programmverwaltung

Anwendungsverwaltung über eine lokale Schnittstelle.

Ereignis-Datenverwaltung

Ein Teil der Administrationsserver-Datenbank, der Speicherung von Informationen über Ereignisse im Kaspersky Next Expert View 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.

Geräte-Tag

Eine Bezeichnung für ein Gerät, die zur Gruppierung, Beschreibung oder Suche von Geräten verwendet werden kann.

Gerätebesitzer

Der Gerätebesitzer ist ein Benutzer, an den sich der Administrator wenden kann, wenn Bedarf zur Durchführung bestimmter Operationen auf einem Gerät besteht.

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.

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, das die Verwaltung über Kaspersky Next Expert View nicht unterstützt.

Installationspaket

Ein Satz von Dateien, der für die Remote-Installation einer Kaspersky-Anwendung mithilfe des Remote-Verwaltungssystems von Kaspersky Next Expert View 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.

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 Next Expert View Administrator

Person, die Programmvorgänge über das zentralisierte Remote-Verwaltungssystem Kaspersky Next Expert View verwaltet.

Kaspersky Next Expert View Operator

Benutzer, der den Status und Betrieb eines Schutzsystems überwacht, das mithilfe von Kaspersky Next Expert View verwaltet wird.

Kaspersky Next Pro View

Diese Anwendung dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentralisiert zu erledigen. Kaspersky Next Expert View wird durch Kaspersky gehostet und gewartet. Die Anwendung ist ein Teil der Cloud-Lösung Kaspersky Next. Innerhalb dieser Lösung können Sie auch Kaspersky Next Pro View verwenden.

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 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 Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.

Konto in Kaspersky Next Expert View

Ein Benutzerkonto, das Sie haben müssen, um Kaspersky Next Expert View beispielsweise durch das Anlegen und Löschen von Benutzerkonten und das Einstellen von Sicherheitsprofilen (Sicherheitsrichtlinien) zu konfigurieren. Mit diesem Konto können Sie den Dienst My Kaspersky verwenden. Sie erstellen dieses Konto, wenn Sie Kaspersky Next Expert View verwenden.

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.

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.

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.

Programm-Tag

Eine Bezeichnung für Programme von Drittanbietern, anhand derer die Programme gruppiert und gefunden werden können. Einem Programm zugewiesene Tags können als Bedingung für Geräteauswahlen angegeben werden.

Programmeinstellungen

Anwendungseinstellungen, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb der Anwendung regeln, zum Beispiel Leistungseinstellungen, Berichtseinstellungen und Backup-Einstellungen.

Push-Server

Eine Funktion des Verteilungspunkts, die es Ihnen ermöglicht, eine permanente Verbindung zwischen den verwalteten Geräten und dem Administrationsserver aufrechtzuerhalten. Dies ist erforderlich, um Informationen von den Geräten abzurufen und Befehle zur Verwaltung der Geräte umgehend auszuführen.

Quarantäne

Ein spezieller Speicher, in den Dateien verschoben werden, die möglicherweise von Viren infiziert oder im Augenblick des Fundes irreparabel sind.

Remote-Installation

Installation von Kaspersky-Anwendungen mithilfe der von Kaspersky Next Expert View 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 Programme, die auf Computern in mehreren Administrationsgruppen installiert sind, erstellen, es kann jedoch innerhalb einer Administrationsgruppe immer nur eine Richtlinie auf ein Programm angewendet werden.

Richtlinienprofil

Eine benannte Teilmenge der Richtlinieneinstellungen. Diese Teilmenge wird auf den Zielgeräten zusammen mit der Richtlinie verteilt und ergänzt diese unter einer bestimmten, als Profilaktivierungsbedingung bezeichneten, Umständen.

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.

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.

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

Zusammenstellung von Modul-Updates Kaspersky-Anwendungen einschließlich kritischer Updates, die sich über einen bestimmten Zeitraum angesammelt haben.

Verteilungspunkt

Computer, auf dem der Administrationsagent installiert ist und der zur Update-Verteilung, Netzwerkabfrage, Remote-Installation von Programmen und zum Empfangen von Informationen über Computer in einer Administrationsgruppe und/oder Broadcasting-Domäne verwendet wird. Der Administrator wählt die entsprechenden Geräte aus und weist sie manuell als Verteilungspunkte zu. Verteilungspunkte können auch als Verbindungs-Gateways fungieren, um die Anzahl der ausgehenden externen Verbindungen und der gleichzeitigen Verbindungen zum Administrationsserver zu reduzieren. Es wird empfohlen, die Anzahl der verwalteten Computer zu begrenzen, die sich direkt mit dem Administrationsserver verbinden.

Verwaltetes Gerät

Computer mit installiertem Administrationsagenten oder mobiles Gerät mit einer installierten Kaspersky-Sicherheitsanwendung.

Virenangriff

Eine Serie von vorsätzlichen Versuchen, ein Gerät mit einem Virus zu infizieren.

Virtueller Administrationsserver

Eine Komponente von Kaspersky Next Expert View, 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 als sekundärer Administrationsserver fungieren.
- Für virtuelle Administrationsserver können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).

Web-Plug-ins zur Verwaltung

Eine spezielle Komponente zur Remote-Verwaltung von Kaspersky-Programmen mittels von Kaspersky Next Expert View. Das Verwaltungs-Plug-in ist eine Schnittstelle zwischen Kaspersky Next Expert View und einer spezifischen Kaspersky-Anwendung. Mit einem Verwaltungs-Plug-in können Sie Aufgaben und Richtlinien für die Anwendung konfigurieren.

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.

Zentralisierte Programmverwaltung

Remote-Programmverwaltung mithilfe der Verwaltungsdienste, die in Kaspersky Next Expert View bereitgestellt werden.

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 Datei "legal_notices.txt" befindet sich ebenfalls im Installationsordner der verwalteten Anwendungen.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash, PostScript, Reader und Shockwave sind in den USA und/oder anderen Ländern entweder eingetragene Markenzeichen oder Markenzeichen von Adobe.

AMD64 ist Markenzeichen oder ein eingetragenes Markenzeichen von Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS 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, App Store, AppleScript, FileVault, iPadOS, iPhone, iTunes, Mac, Mac OS, macOS, OS X, Safari und QuickTime 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, IOS und Cisco Jabber sind eingetragene Markenzeichen oder 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.

Cloudflare, das Cloudflare-Logo und Cloudflare Workers sind Markenzeichen und/oder eingetragene Markenzeichen von Cloudflare, Inc. in den USA und anderen Gerichtsbarkeiten.

Corel und CorelDRAW sind Markenzeichen oder eingetragene Markenzeichen der Corel Corporation und/oder ihrer Tochtergesellschaften in Kanada, den USA und/oder anderen Ländern.

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 Markenzeichen der The FreeBSD Foundation.

Google, Android, Chrome, Dalvik, Firebase, Google Chrome, Google Earth, Google Maps, Google Play und Google Public DNS sind Markenzeichen von Google LLC.

HUAWEI, EulerOS, HUAWEI CLOUD sind Marken von Huawei Technologies Co., Ltd.

Intel und Core 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, ActiveX, BitLocker, Excel, Hyper-V, InfoPath, Internet Explorer, Microsoft 365, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Azure, Windows Media, Windows Mobile, Windows Phone, Windows Server und Windows Vista 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.

Oracle, Java und JavaScript 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.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Red Hat, Red Hat Enterprise Linux und CentOS, Fedora sind in den USA und in anderen Ländern 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.

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 ist ein Markenzeichen und ein eingetragenes 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.

Rocky Linux ist ein Markenzeichen der The Rocky Enterprise Software Foundation.

UNIX ist ein in den USA und in anderen Ländern eingetragenes Markenzeichen, welches exklusiv durch die X/Open Company Limited lizenziert wird.